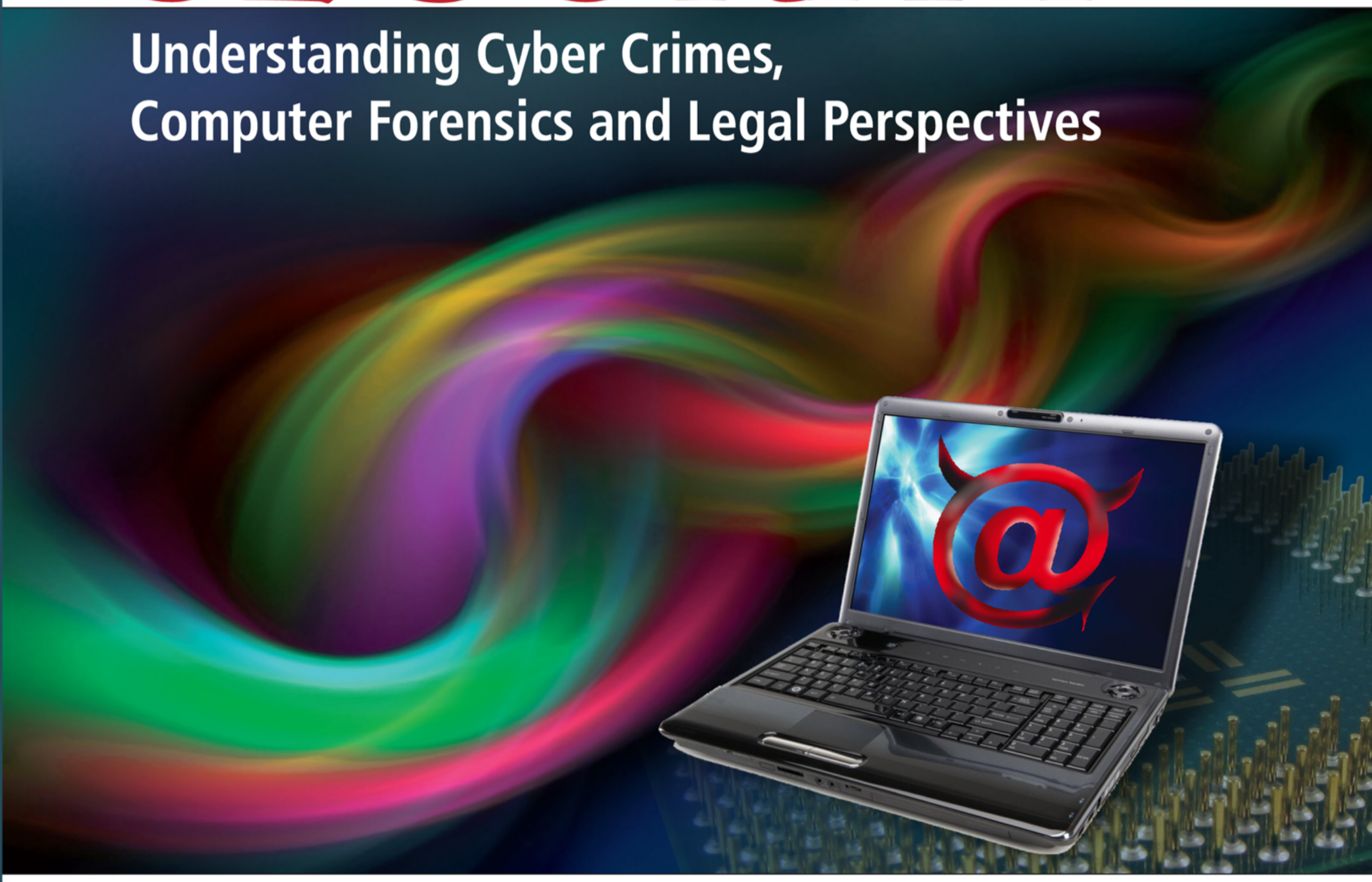
Foreword by
Dr. Kamlesh Bajaj, Data Security Council of India

WILEY-INDIA

CYBER SECURITY

Understanding Cyber Crimes, Computer Forensics and Legal Perspectives



Nina Godbole • Sunit Belapure

Contents

Foreword vii
About Dr. Kamlesh Bajaj ix
About the Authors xi
Preface xiii
Acknowledgments xvii
List of Figures xxxiii
List of Tables xxxix
List of Boxes xliii

1 Introduction to Cybercrime 1

Learning Objectives 1
1.1 Introduction 1
1.2 Cybercrime: Definition and Origins of the Word 1
1.3 Cybercrime and Information Security 13
1.4 Who are Cybercriminals? 16
1.5 Classifications of Cybercrimes 17
1.5.1 E-Mail Spoofing 18
1.5.2 Spamming 18
1.5.3 Cyberdefamation 19
1.5.4 Internet Time Theft 21
1.5.5 Salami Attack/Salami Technique 21
1.5.6 Data Diddling 21
1.5.7 Forgery 22
1.5.8 Web Jacking 22
1.5.9 Newsgroup Spam/Crimes Emanating from Usenet Newsgroup 22
1.5.10 Industrial Spying/Industrial Espionage 22
1.5.11 Hacking 23
1.5.12 Online Frauds 23
1.5.13 Pornographic Offenses 27
1.5.14 Software Piracy 28
1.5.15 Computer Sabotage 28
1.5.16 E-Mail Bombing/Mail Bombs 30
1.5.17 Usenet Newsgroup as the Source of Cybercrimes 30
1.5.18 Computer Network Intrusions 30
1.5.19 Password Sniffing 30
1.5.20 Credit Card Frauds 31
1.5.21 Identity Theft 31
1.6 Cybercrime: The Legal Perspectives 32
1.7 Cybercrimes: An Indian Perspective 32

1.8	Cybercrime and the Indian ITA 2000	34
	1.8.1 Hacking and the Indian Law(s)	34
1.9	A Global Perspective on Cybercrimes	36
	1.9.1 Cybercrime and the Extended Enterprise	38
1.10	Cybercrime Era: Survival Mantra for the Netizens	39
1.11	Concluding Remarks and Way Forward to Further Chapters	39
	Summary	40
	Review Questions	40
	References	40
	Further Reading	42
2	**Cyberoffenses: How Criminals Plan Them**	**45**
	Learning Objectives	45
2.1	Introduction	45
	2.1.1 Categories of Cybercrime	48
2.2	How Criminals Plan the Attacks	49
	2.2.1 Reconnaissance	50
	2.2.2 Passive Attacks	50
	2.2.3 Active Attacks	54
	2.2.4 Scanning and Scrutinizing Gathered Information	58
	2.2.5 Attack (Gaining and Maintaining the System Access)	61
2.3	Social Engineering	61
	2.3.1 Classification of Social Engineering	62
2.4	Cyberstalking	65
	2.4.1 Types of Stalkers	66
	2.4.2 Cases Reported on Cyberstalking	66
	2.4.3 How Stalking Works?	66
	2.4.4 Real-Life Incident of Cyberstalking	67
2.5	Cybercafe and Cybercrimes	67
2.6	Botnets: The Fuel for Cybercrime	71
	2.6.1 Botnet	71
2.7	Attack Vector	73
2.8	Cloud Computing	75
	2.8.1 Why Cloud Computing?	76
	2.8.2 Types of Services	77
	2.8.3 Cybercrime and Cloud Computing	77
	Summary	79
	Review Questions	79
	References	79
	Further Reading	80
3	**Cybercrime: Mobile and Wireless Devices**	**81**
	Learning Objectives	81
3.1	Introduction	81
3.2	Proliferation of Mobile and Wireless Devices	82

3.3	Trends in Mobility	84
3.4	Credit Card Frauds in Mobile and Wireless Computing Era	87
	3.4.1 Types and Techniques of Credit Card Frauds	88
3.5	Security Challenges Posed by Mobile Devices	91
3.6	Registry Settings for Mobile Devices	92
3.7	Authentication Service Security	93
	3.7.1 Cryptographic Security for Mobile Devices	93
	3.7.2 LDAP Security for Hand-Held Mobile Computing Devices	94
	3.7.3 RAS Security for Mobile Devices	95
	3.7.4 Media Player Control Security	98
	3.7.5 Networking API Security for Mobile Computing Applications	98
3.8	Attacks on Mobile/Cell Phones	99
	3.8.1 Mobile Phone Theft	99
	3.8.2 Mobile Viruses	101
	3.8.3 Mishing	101
	3.8.4 Vishing	102
	3.8.5 Smishing	103
	3.8.6 Hacking Bluetooth	105
3.9	Mobile Devices: Security Implications for Organizations	107
	3.9.1 Managing Diversity and Proliferation of Hand-Held Devices	107
	3.9.2 Unconventional/Stealth Storage Devices	108
	3.9.3 Threats through Lost and Stolen Devices	110
	3.9.4 Protecting Data on Lost Devices	111
	3.9.5 Educating the Laptop Users	111
3.10	Organizational Measures for Handling Mobile Devices-Related Security Issues	112
	3.10.1 Encrypting Organizational Databases	113
	3.10.2 Including Mobile Devices in Security Strategy	113
3.11	Organizational Security Policies and Measures in Mobile Computing Era	114
	3.11.1 Importance of Security Policies relating to Mobile Computing Devices	114
	3.11.2 Operating Guidelines for Implementing Mobile Device Security Policies	115
	3.11.3 Organizational Policies for the Use of Mobile Hand-Held Devices	116
3.12	Laptops	116
	3.12.1 Physical Security Countermeasures	117
	Summary	120
	Review Questions	121
	References	121
	Further Reading	122

4	**Tools and Methods Used in Cybercrime**	**125**
	Learning Objectives	125
4.1	Introduction	125
4.2	Proxy Servers and Anonymizers	129

4.3	Phishing	131
	4.3.1 How Phishing Works?	131
4.4	Password Cracking	132
	4.4.1 Online Attacks	134
	4.4.2 Offline Attacks	134
	4.4.3 Strong, Weak and Random Passwords	135
	4.4.4 Random Passwords	136
4.5	Keyloggers and Spywares	137
	4.5.1 Software Keyloggers	137
	4.5.2 Hardware Keyloggers	140
	4.5.3 Antikeylogger	140
	4.5.4 Spywares	140
4.6	Virus and Worms	143
	4.6.1 Types of Viruses	146
4.7	Trojan Horses and Backdoors	151
	4.7.1 Backdoor	152
	4.7.2 How to Protect from Trojan Horses and Backdoors	153
4.8	Steganography	155
	4.8.1 Steganalysis	158
4.9	DoS and DDoS Attacks	158
	4.9.1 DoS Attacks	158
	4.9.2 Classification of DoS Attacks	159
	4.9.3 Types or Levels of DoS Attacks	160
	4.9.4 Tools Used to Launch DoS Attack	161
	4.9.5 DDoS Attacks	162
	4.9.6 How to Protect from DoS/DDoS Attacks	163
4.10	SQL Injection	164
	4.10.1 Steps for SQL Injection Attack	165
	4.10.2 How to Prevent SQL Injection Attacks	167
4.11	Buffer Overflow	168
	4.11.1 Types of Buffer Overflow	168
	4.11.2 How to Minimize Buffer Overflow	170
4.12	Attacks on Wireless Networks	171
	4.12.1 Traditional Techniques of Attacks on Wireless Networks	176
	4.12.2 Theft of Internet Hours and Wi-Fi-based Frauds and Misuses	177
	4.12.3 How to Secure the Wireless Networks	179
	Summary	180
	Review Questions	181
	References	181
	Further Reading	183

5	**Phishing and Identity Theft**	**185**
	Learning Objectives	185
5.1	Introduction	185

5.2 Phishing 187
5.2.1 Methods of Phishing 191
5.2.2 Phishing Techniques 193
5.2.3 Spear Phishing 195
5.2.4 Types of Phishing Scams 196
5.2.5 Phishing Toolkits and Spy Phishing 201
5.2.6 Phishing Countermeasures 202
5.3 Identity Theft (ID Theft) 206
5.3.1 Personally Identifiable Information(PII) 209
5.3.2 Types of Identity Theft 211
5.3.3 Techniques of ID Theft 218
5.3.4 Identity Theft: Countermeasures 220
5.3.5 How to Efface Your Online Identity 220
Summary 221
Review Questions 222
References 222
Further Reading 224

6 Cybercrimes and Cybersecurity: The Legal Perspectives 227

Learning Objectives 227
6.1 Introduction 227
6.2 Cybercrime and the Legal Landscape around the World 230
6.2.1 A Broad View on Cybercrime Law Scenario in the Asia-Pacific Region 231
6.2.2 Online Safety and Cybercrime Laws: Detailed Perspective on the Current Asia-Pacific Scenario 233
6.2.3 Anti-Spam Laws in Canada 243
6.2.4 Cybercrime and Federal Laws in the US 245
6.2.5 The EU Legal Framework for Information Privacy to Prevent Cybercrime 247
6.2.6 Cybercrime Legislation in the African Region 249
6.3 Why Do We Need Cyberlaws: The Indian Context 253
6.4 The Indian IT Act 254
6.4.1 Admissibility of Electronic Records: Amendments made in the Indian ITA 2000 264
6.4.2 Positive Aspects of the ITA 2000 269
6.4.3 Weak Areas of the ITA 2000 270
6.5 Challenges to Indian Law and Cybercrime Scenario in India 271
6.6 Consequences of Not Addressing the Weakness in Information Technology Act 272
6.7 Digital Signatures and the Indian IT Act 273
6.7.1 Public-Key Certificate 273
6.7.2 Representation of Digital Signatures in the ITA 2000 274
6.7.3 Impact of Oversights in ITA 2000 Regarding Digital Signatures 275
6.7.4 Implications for Certifying Authorities 277

	6.7.5 The Current Scenario Regarding Digital Signatures under the Indian IT Act	278
	6.7.6 Cryptographic Perspective on the Indian IT Act	279
6.8	Amendments to the Indian IT Act	282
	6.8.1 Overview of Changes Made to the Indian IT Act	283
	6.8.2 Cybercafe-Related Matters Addressed in the Amendment to the Indian IT Act	289
	6.8.3 State Government Powers Impacted by the Amendments to the Indian IT Act	293
	6.8.4 Impact of IT Act Amendments on Information Technology Organizations	295
6.9	Cybercrime and Punishment	305
6.10	Cyberlaw, Technology and Students: Indian Scenario	307
	Summary	309
	Review Questions	310
	References	311
	Further Reading	312

7 Understanding Computer Forensics 317

	Learning Objectives	317
7.1	Introduction	317
7.2	Historical Background of Cyberforensics	318
7.3	Digital Forensics Science	320
7.4	The Need for Computer Forensics	323
7.5	Cyberforensics and Digital Evidence	327
	7.5.1 The Rules of Evidence	329
7.6	Forensics Analysis of E-Mail	332
	7.6.1 RFC2822	338
7.7	Digital Forensics Life Cycle	339
	7.7.1 The Digital Forensics Process	339
	7.7.2 The Phases in Computer Forensics/Digital Forensics	341
	7.7.3 Precautions to be Taken when Collecting Electronic Evidence	353
7.8	Chain of Custody Concept	355
7.9	Network Forensics	357
7.10	Approaching a Computer Forensics Investigation	358
	7.10.1 Typical Elements Addressed in a Forensics Investigation Engagement Contract	359
	7.10.2 Solving a Computer Forensics Case	361
7.11	Setting up a Computer Forensics Laboratory: Understanding the Requirements	362
7.12	Computer Forensics and Steganography	368
	7.12.1 Rootkits	370
	7.12.2 Information Hiding	371
7.13	Relevance of the OSI 7 Layer Model to Computer Forensics	373
	7.13.1 Step 1: Foot Printing	373

7.13.2 Step 2: Scanning and Probing 375
7.13.3 Step 3: Gaining Access 376
7.13.4 Step 4: Privilege 376
7.13.5 Step 5: Exploit 376
7.13.6 Step 6: Retracting 376
7.13.7 Step 7: Installing Backdoors 376
7.14 Forensics and Social Networking Sites: The Security/Privacy Threats 377
7.15 Computer Forensics from Compliance Perspective 383
7.15.1 The Regulatory Perspective for Forensics at the International Level 384
7.15.2 Computer Forensics Compliance Requirements: Implications for Evidential Aspects 388
7.15.3 Computer Forensics Expertise Status in India 389
7.16 Challenges in Computer Forensics 389
7.16.1 Technical Challenges: Understanding the Raw Data and its Structure 390
7.16.2 The Legal Challenges in Computer Forensics and Data Privacy Issues 392
7.17 Special Tools and Techniques 396
7.17.1 Digital Forensics Tools Ready Reckenor 397
7.17.2 Special Technique: Data Mining used in Cyberforensics 402
7.18 Forensics Auditing 403
7.19 Antiforensics 406
Summary 408
Review Questions 409
References 410
Further Reading 415

8 Forensics of Hand-Held Devices 423

Learning Objectives 423
8.1 Introduction 423
8.2 Understanding Cell Phone Working Characteristics 425
8.2.1 Understanding the Types of Cellular Networks 426
8.2.2 NTT DoCoMo 428
8.2.3 Cell Phones: Hardware and Software Features 430
8.3 Hand-Held Devices and Digital Forensics 431
8.3.1 Mobile Phone Forensics 433
8.3.2 PDA Forensics 438
8.3.3 Printer Forensics 440
8.3.4 Scanner Forensics 442
8.3.5 Smartphone Forensics 442
8.3.6 iPhone Forensics 445
8.3.7 Challenges in Forensics of the Digital Images and Still Camera 454
8.3.8 Forensics of the BlackBerry Wireless Device 458
8.4 Toolkits for Hand-Held Device Forensics 463
8.4.1 EnCase 464

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.

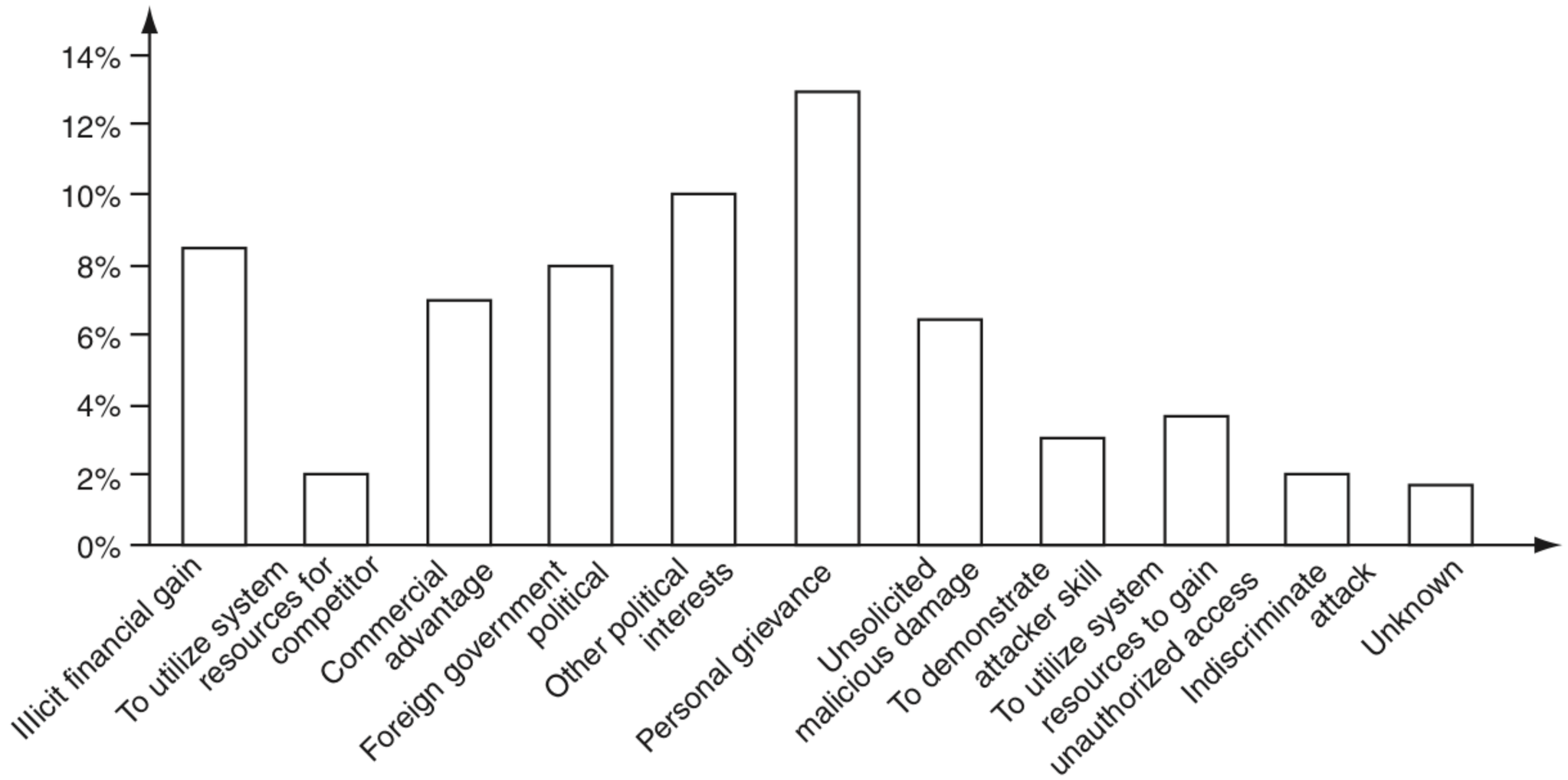


Figure 1.1 Cybercrime trend.
Source: 2008 Pacific Islands Computer Crime and Security Survey. Adapted from *Cybercrime: Threats, Challenges* presentation by Wipul Jayawickrama at the Computer Security Week 2008 in Brisbane, Australia (reproduced with permission).

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 under IPC 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	0	0	0	0	—	0	0	0	0	—
4	Forgery	77	48	160	217	35.6	81	71	194	264	36.1
5	Criminal breach of trust/ fraud	173	186	90	73	–18.9	181	215	121	85	–29.8
6	Counterfeiting										
	(i) Property/ mark	12	0	13	8	–38.5	8	0	7	23	228.6
	(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*	*EveTeasing/ 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

(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*	*EveTeasing/ 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

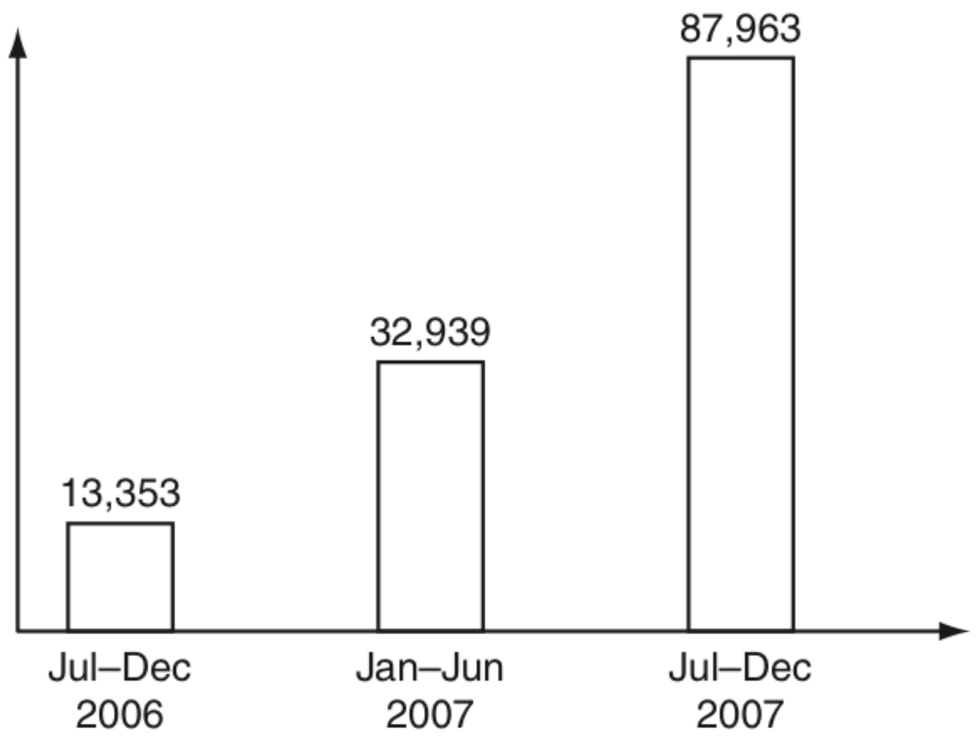


Figure 1.2 Rise in the number of Phishing hosts.
Source: Symantec (International Telecommunications Society, 17th Biennial Conference, Montreal, Canada, June 24–27, 2008).

their unlawful act to gain information which can result in heavy loss/damage to the owner of that intangible sensitive information. [See Further Reading, Books, Ref. #3 for a pointer to data privacy and understanding terms such as sensitive information, personal information (PI) and sensitive personal information (SPI).] Internet is one of the means by which the offenders can gain priced sensitive information of companies, firms, individuals, banks and can lead to intellectual property (IP) crimes (such as stealing new product plans, its description, market program plans, list of customers, etc.), selling illegal articles, pornography/child pornography, etc. This is done using methods such as Phishing, Spoofing, Pharming, Internet Phishing, wire transfer, etc. and use it to their own advantage without the consent of the individual. "Phishing" refers to an attack using mail programs to deceive or coax Internet users into disclosing confidential information that can be then exploited for illegal purposes. Figure 1.2 shows the increase in Phishing hosts.

1.3 Cybercrime and Information Security

Lack of information security gives rise to cybercrimes. This subject is explained in greater detail in Chapter 9. Let us refer to the amended Indian Information Technology Act (ITA) 2000[7] in the context of cybercrime. From an Indian perspective, the new version of the Act (referred to as *ITA 2008*) provides a new focus on "Information Security in India." "Cybersecurity" means protecting information, equipment, devices, computer, computer resource, communication device and information stored therein from unauthorized access, use, disclosure, disruption, modification or destruction. The term incorporates both the physical security of devices as well as the information stored therein. It covers protection from unauthorized access, use, disclosure, disruption, modification and destruction. (For a thorough discussion about these aspects, see Ref. #2, Books, Further Reading.

Where financial losses to the organization due to insider crimes are concerned (e.g., leaking customer data), often some difficulty is faced in estimating the losses because the financial impacts may not be detected by the victimized organization and no direct costs may be associated with the data theft. The 2008 CSI Survey[8] on computer crime and security supports this. Cybercrimes occupy an important space in information security domain because of their impact. For anyone trying to compile data on business impact of cybercrime, there are number of challenges. One of them comes from the fact that organizations do not explicitly incorporate the cost of the vast majority of computer security incidents into their accounting as opposed to, say,

Box 1.2 The Botnet Menace!

The topic of Botnets is discussed in Section 2.6, Chapter 2. The term "Botnet" is used to refer to a group of compromised computers (zombie computers, i.e., personal computers secretly under the control of hackers) running malwares under a common command and control infrastructure. Figure 1.3 shows how a "zombie" works.

A Botnet maker can control the group remotely for illegal purposes, the most common being denial-of-service attack (DoS attack), Adware, Spyware, E-Mail Spam, Click Fraud (see reference links provided in Ref. #5, Articles and Research Papers, Further Reading), theft of application serial numbers, login IDs and financial information such as credit card numbers, etc. An attacker usually gains control by infecting the computers with a virus or other Malicious Code. The computer may continue to operate normally without the owner's knowledge that his computer has been compromised. The topic of computer viruses is addressed in Chapter 4 (Section 4.6).

The problem of Botnet is global in nature and India is also facing the same. India has an average of 374 new Bot attacks per day and had more than 38,000 distinct Bot-infected computers in the first half of the year 2009. Small and medium businesses in the country are at greater risk, as they are highly vulnerable to Bots, Phishing, Spam and Malicious Code attacks. Mumbai with 33% incidences tops the Bot-infected city list, followed by New Delhi at 25%, Chennai at 17% and Bangalore at 13%. Tier-II locations are now also a target of Bot-networks with Bhopal at 4% and Hyderabad, Surat, Pune and Noida at 1% each.

The Internet is a network of interconnected computers. If the computers, computer systems, computer resources, etc. are unsecured and vulnerable to security threats, it can be detrimental to the critical infrastructure of the country. We have witnessed the incidence of Cyberwar against Estonia and the same is possible against any country including India.

Source: Nina Godbole (2009), *Information Systems Security: Security Management, Metrics, Frameworks and Best Practices*, Wiley India (Chapter 3, Section 3.7, Fig. 3.8).

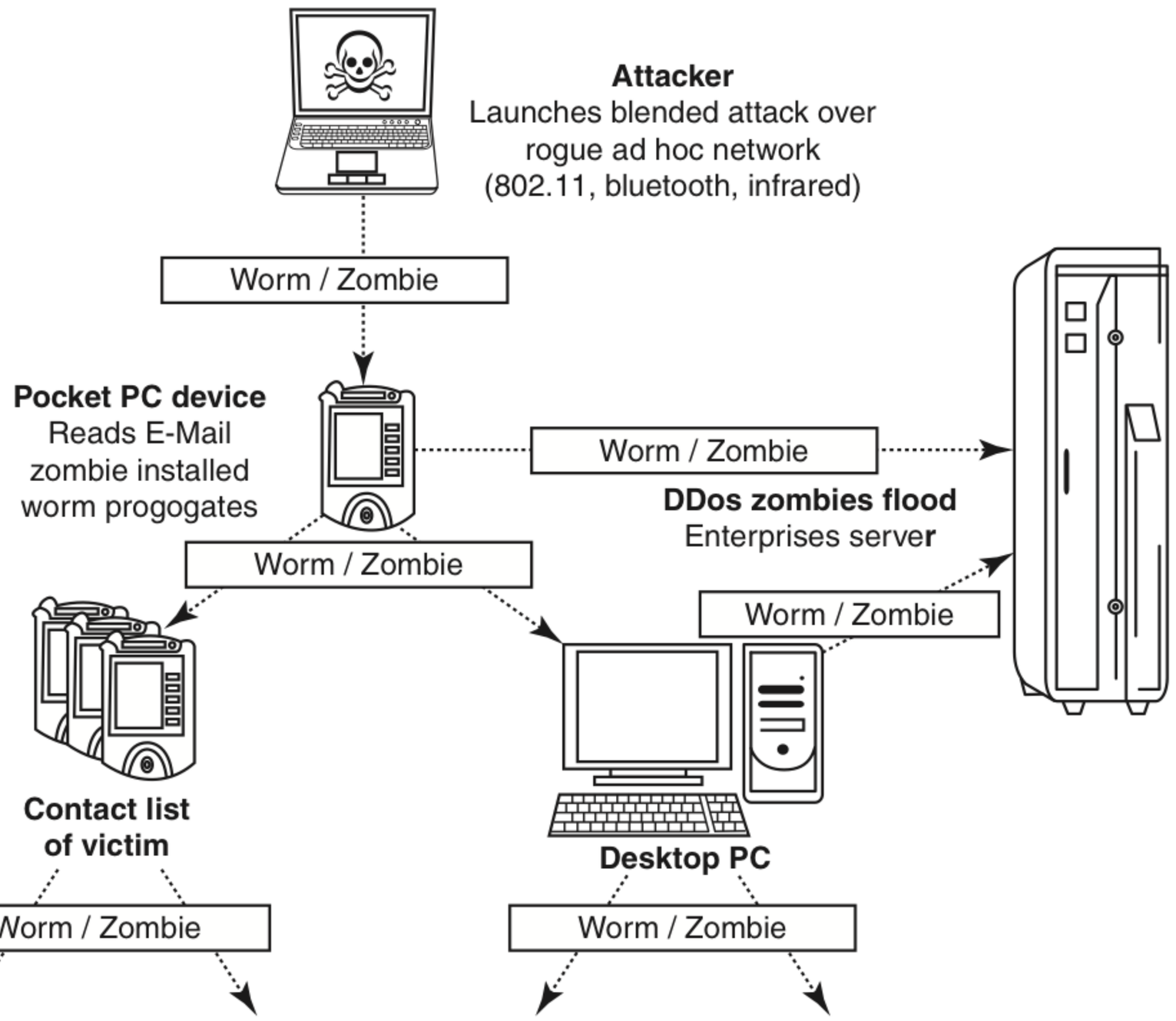


Figure 1.3 | How a zombie works.

accounting for the "shrinkage" of goods from retail stores. The other challenge comes from the difficulty in attaching a quantifiable monetary value to the corporate data and yet corporate data get stolen/lost (most notably through loss/theft of laptops, see the survey conducted by Ponemon Institute in Ref. #19, Additional Useful Web References, Further Reading). Because of these reasons, reporting of financial losses often remains approximate. In an attempt to avoid negative publicity, most organizations abstain from revealing facts and figures about "security incidents" including cybercrime. In general, organizations perception about "insider attacks" seems to be different than that made out by security solution vendor. However, this perception of an organization does not seem to be true as revealed by the 2008 CSI Survey. Awareness about "data privacy" too tends to be low in most organizations. When we speak of financial losses to the organization and significant insider crimes, such as leaking customer data, such "crimes" may not be detected by the victimized organization and no direct costs may be associated with the theft (Table 1.5).

Figure 1.4 shows several categories of incidences – *viruses*, *insider abuse*, *laptop theft* and *unauthorized access* to systems. Refer to Ref. #1 (Chapter 3, Section 3.11), Book, Further Reading for laptop threats and information security implications in mobile computing paradigm and "thefts/losses." Also read Chapter 9 of this book.

Typical network misuses are for Internet radio/streaming audio, streaming video, file sharing, instant messaging and online gaming (such as online poker, online casinos, online betting, etc.; refer to http://

Table 1.5 | Cybercrime trend over the years (1999–2008)

Types of Cybercrime	*2004 (%)*	*2005 (%)*	*2006 (%)*	*2007 (%)*	*2008 (%)*
Denial of service (DoS)	39	32	25	25	21
Laptop theft	49	48	47	50	42
Telecom fraud	10	10	8	5	5
Unauthorized access	37	32	32	25	29
Viruses (addressed in Chapter 4)	78	74	65	52	50
Financial fraud	8	7	9	12	12
Insider abuse	59	48	42	59	44
System penetration	17	14	15	13	13
Sabotage	5	2	3	4	2
Theft/loss of proprietary information	10	9	9	8	9
• from mobile devices					4
• from all other sources					5
Website defacement (see Figs. 1.6–1.10)	7	5	6	10	6
Abuse of wireless network	15	16	14	17	14
Misuse of web application	10	5	6	9	11
Bots (see Box 1.2; more in Chapter 2)				21	20
DoS attacks				6	8
Instant messaging abuse				25	21
Password sniffing (explained in Chapter 2)				10	9
Theft/loss of customer data				17	17
• from mobile devices					8
• from all other sources					8

Source: 2008 CSI Computer Crime and Security Survey available at the link http://i.cmpnet.com/v2.gocsi.com/pdf/CSIsurvey2008.pdf (15 March 2009).

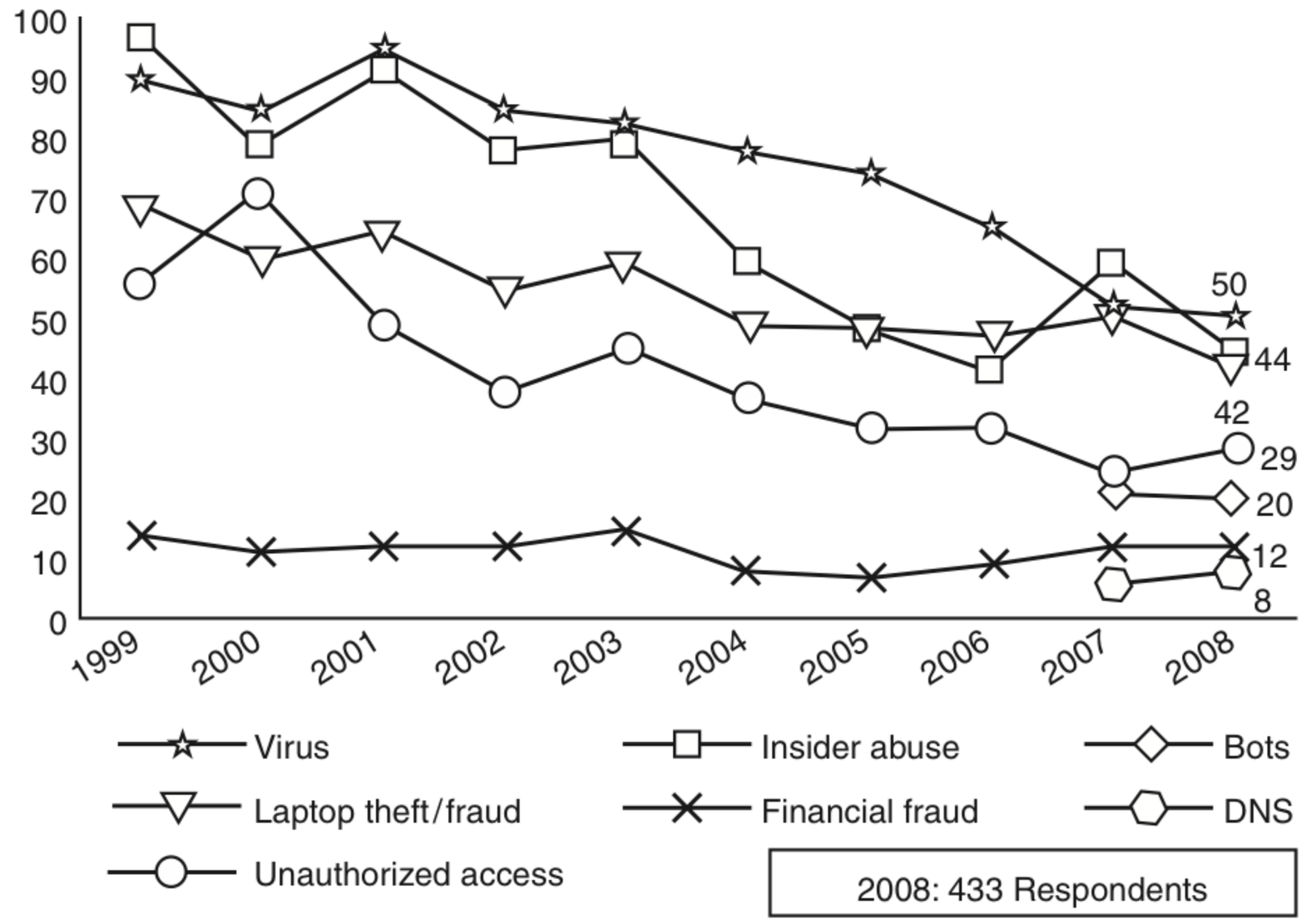


Figure 1.4 Major types of incidents by percentage.
Source: 2008 CSI Computer Crime and Security Survey available at the link http://i.cmpnet.com/v2.gocsi.com/pdf/CSIsurvey2008.pdf (15 March 2009).

en.wikipedia.org/wiki/Online_gambling). Online gambling is illegal in some countries – for example, in India. However, India has yet to pass laws that specifically deal with the issue, leaving a sort of legal loophole in the meantime. (In Ref. #20, Additional Useful Web References, Further Reading, we have provided links to refer to about legal status of online gambling in India. The Indian online gambling market is estimated to be worth 1–5 billion US$!)

1.4 Who are Cybercriminals?

Cybercrime involves such activities as child pornography; credit card fraud; cyberstalking; defaming another online; gaining unauthorized access to computer systems; ignoring copyright, software licensing and trademark protection; overriding encryption to make illegal copies; software piracy and stealing another's identity (known as identity theft) to perform criminal acts (see detailed discussion on identity theft in Chapter 5). Cybercriminals are those who conduct such acts. They can be categorized into three groups that reflect their motivation (see Ref. #2, Books, Further Reading):

1. **Type I: Cybercriminals – hungry for recognition**
   - Hobby hackers;
   - IT professionals (social engineering is one of the biggest threat);
   - politically motivated hackers;
   - terrorist organizations.
2. **Type II: Cybercriminals – not interested in recognition**
   - Psychological perverts;
   - financially motivated hackers (corporate espionage);

- state-sponsored hacking (national espionage, sabotage);
- organized criminals.

3. **Type III: Cybercriminals – the insiders**
   - Disgruntled or former employees seeking revenge;
   - competing companies using employees to gain economic advantage through damage and/or theft.

Thus, the typical "motives" behind cybercrime seem to be greed, desire to gain power and/or publicity, desire for revenge, a sense of adventure, looking for thrill to access forbidden information, destructive mindset and desire to sell network security services. This is explained in Chapter 10. Cybercafes are known to play role in committing cybercrimes. A link about cybercafes under ITA 2008 (amendment to Indian ITA 2000) is provided in Ref. #23, Additional Useful Web References, Further Reading. Another link, describing views if the amended ITA 2000 is stringent enough for cybercriminals, is provided in the same section as Ref. #24.

1.5 Classifications of Cybercrimes

Table 1.6 presents a scheme for cybercrime classification (broad and narrow classification).

Crime is defined as "*an act or the commission of an act that is forbidden, or the omission of a duty that is commanded by a public law and that makes the offender liable to punishment by that law*" (Webster Dictionary). Cybercrimes are classified as follows:

1. **Cybercrime against individual**
   - *Electronic mail* (*E-Mail*) *Spoofing and other online frauds:* Refer to Section 1.5.1 of this chapter and Chapter 4 for more details.
   - *Phishing, Spear Phishing* and its various other forms such as Vishing (Section 3.8.4) and Smishing (Section 3.8.5): Refer to Chapter 5 for discussion about Phishing and Spear Phishing.
   - *Spamming:* It is explained in Section 1.5.2.
   - *Cyberdefamation:* It is explained later in Section 1.5.3.
   - *Cyberstalking and harassment:* It is explained in Chapter 2.
   - *Computer sabotage:* It is explained later in Section 1.5.15.
   - *Pornographic offenses:* It is explained in Section 1.5.13.
   - *Password sniffing:* This also belongs to the category of cybercrimes against organization because the use of password could be by an individual for his/her personal work or the work he/she is doing using a computer that belongs to an organization. It is explained in Section 1.5.19 (also see Table 1.5).

Table 1.6 | Classifying cybercrimes – broad and narrow

	Cybercrime in Narrow Sense	*Cybercrime in Broad Sense*	
Role of computer	*Computer as an object* The computer/information stored on the computer is the subject/target of the crime	*Computer as a tool* The computer/or information stored on the computer constitutes an important tool for committing the crime	*Computer as the environment or context* The computer/information stored on the computer plays a non-substantial role in the act of crime, but does contain evidence of the crime
Examples	Hacking, computer sabotage, DDoS-attacks (distributed denial-of-service attacks), virtual child pornography	Computer fraud, forgery distribution of child pornography	Murder using computer techniques, bank robbery and drugs trade

2. **Cybercrime against property**
   - *Credit card frauds:* Refer to Chapter 5 for Phishing and Spear Phishing and Chapter 11, Section 11.4 (in CD).
   - *Intellectual property (IP) crimes:* Basically, IP crimes include software piracy, copyright infringement, trademarks violations, theft of computer source code, etc. (refer to Chapters 9 and 10).
   - *Internet time theft:* It is explained in Section 1.5.4 as well as in Chapter 11 (Mini-Case 4, Section 11.3.4).
3. **Cybercrime against organization**
   - *Unauthorized accessing of computer:* Hacking is one method of doing this and hacking is a punishable offense (see point 2 in Box 1.7).
   - *Password sniffing:* It is explained in Section 1.5.19 (also see Table 1.5).
   - *Denial-of-service attacks* (known as DoS attacks)*:* It is explained more in detail in Chapter 4.
   - *Virus attack/dissemination of viruses:* Refer to Chapter 4 for detailed discussion on this.
   - *E-Mail bombing/mail bombs:* It is explained in Section 1.5.16.
   - *Salami attack/Salami technique:* It is explained in Section 1.5.5.
   - *Logic bomb:* It is explained in Section 1.5.15 (Computer Sabotage).
   - *Trojan Horse:* It is explained more in detail in Chapter 4.
   - *Data diddling:* It is explained in Section 1.5.6. Refer to Section 11.2.6, Chapter 11.
   - *Crimes emanating from Usenet newsgroup:* It is explained in Section 1.5.9.
   - *Industrial spying/industrial espionage:* It is explained in Section 1.5.10.
   - *Computer network intrusions:* It is explained in Section 1.5.18.
   - *Software piracy* – It is explained in Section 1.5.14. Also refer to Section 9.2.2, Chapter 9.
4. **Cybercrime against Society**
   - *Forgery:* It is explained in Section 1.5.7 (see Table 1.6 and Box 1.6).
   - *Cyberterrorism:* Refer to Box 1.1 and Box 1.7, and Section 1.2 for detailed discussion on this.
   - *Web jacking:* It is explained in Section 1.5.8.
5. **Crimes emanating from Usenet newsgroup:** By its very nature, Usenet groups may carry very offensive, harmful, inaccurate or otherwise inappropriate material, or in some cases, postings that have been mislabeled or are deceptive in another way. Therefore, it is expected that you will use caution and common sense and exercise proper judgment when using Usenet, as well as use the service at your own risk.

Let us take a brief look at some of the cybercrime forms mentioned above.

1.5.1 E-Mail Spoofing

A spoofed E-Mail is one that appears to originate from one source but actually has been sent from another source. For example, let us say, Roopa has an E-Mail address roopa@asianlaws.org. Let us say her boyfriend Suresh and she happen to have a show down. Then Suresh, having become her enemy, spoofs her E-Mail and sends obscene/vulgar messages to all her acquaintances. Since the E-Mails appear to have originated from Roopa, her friends could take offense and relationships could be spoiled for life. See Box 2.7 in Chapter 2.

1.5.2 Spamming

People who create electronic Spam are called *spammers*. Spam is the abuse of electronic messaging systems (including most broadcast media, digital delivery systems) to send unsolicited bulk messages indiscriminately. Although the most widely recognized form of Spam is E-Mail Spam, the term is applied to similar abuses in other media: instant messaging Spam, Usenet newsgroup Spam, web search engine Spam, Spam in blogs, wiki Spam, online classified ads Spam, mobile phone messaging Spam, Internet forum Spam, junk fax transmissions, social networking Spam, file sharing network Spam, video sharing sites, etc.

Spamming is difficult to control because it has economic viability – advertisers have no operating costs beyond the management of their mailing lists, and it is difficult to hold senders accountable for their mass mailings. Spammers are numerous; the volume of unsolicited mail has become very high because the barrier to entry is low. The costs, such as lost productivity and fraud, are borne by the public and by Internet service providers (ISPs), who are forced to add extra capacity to cope with the deluge. Spamming is widely detested, and has been the subject of legislation in many jurisdictions – for example, the CAN-SPAM Act of 2003.

Another definition of spamming is in the context of "search engine spamming." In this context, spamming is alteration or creation of a document with the intent to deceive an electronic catalog or a filing system. Some web authors use "subversive techniques" to ensure that their site appears more frequently or higher number in returned search results – this is strongly discouraged by search engines and there are fines/penalties associated with the use of such subversive techniques. Those who continually attempt to subvert or Spam the search engines may be permanently excluded from the search index. Therefore, the following web publishing techniques should be avoided:

1. Repeating keywords;
2. use of keywords that do not relate to the content on the site;
3. use of fast meta refresh;
4. redirection;
5. IP Cloaking;
6. use of colored text on the same color background;
7. tiny text usage;
8. duplication of pages with different URLs;
9. hidden links;
10. use of different pages that bridge to the same URL (gateway pages).

Further discussion on each of the above is beyond the scope of this chapter which is meant to be only an overview of cybercrimes.

1.5.3 Cyberdefamation

Cyberdefamation is a cognizable offense.

Let us first understand what the term entails. CHAPTER XXI of the Indian Penal Code (IPC) is about DEFAMATION. In Section 499 of CHAPTER XXI of IPC, regarding "defamation" there is a mention that

> *"Whoever, by words either spoken or intended to be read, or by signs or by visible representations, makes or publishes any imputation concerning any person intending to harm, or knowing or having reason to believe that such imputation will harm, the reputation of such person, is said, except in the cases hereinafter expected, to defame that person."*

Cyberdefamation happens when the above takes place in an electronic form. In other words, "cyberdefamation" occurs when defamation takes place with the help of computers and/or the Internet, for example, someone publishes defamatory matter about someone on a website or sends an E-Mail containing defamatory information to all friends of that person. According to the IPC Section 499:

1. It may amount to defamation to impute anything to a deceased person, if the imputation would harm the reputation of that person if living, and is intended to be hurtful to the feelings of his family or other near relatives.

Box 1.3 Internet: A New Fuel for Defamation?

The Web allows an instant global publication of information at a very low cost. Information, which would not normally be revealed prior to the advent of the Internet, can now be obtained by practically anyone. The relatively low cost of connecting to the Internet and the ease of establishing one's own website means that the opportunity for defamation has increased considerably. Now, on the Internet everyone may be a publisher and may be sued as a publisher. A key feature of the Internet is that users do not have to reveal their true identity to send E-Mail or post messages on bulletin boards. Figure 1.5 shows the humor regarding this on the lighter side. Users are able to communicate and make such postings anonymously or under assumed names.

"Faceless" communication channel is the unique feature brought about by the Internet. Not only that but also people can access the Internet in privacy and seclusion of their own homes or offices. These features of the Internet plus the interactive, responsive nature of communications on the Internet means that now the users are far less inhibited about the contents of their messages resulting in cyberspace becoming excessively prone to defamation.

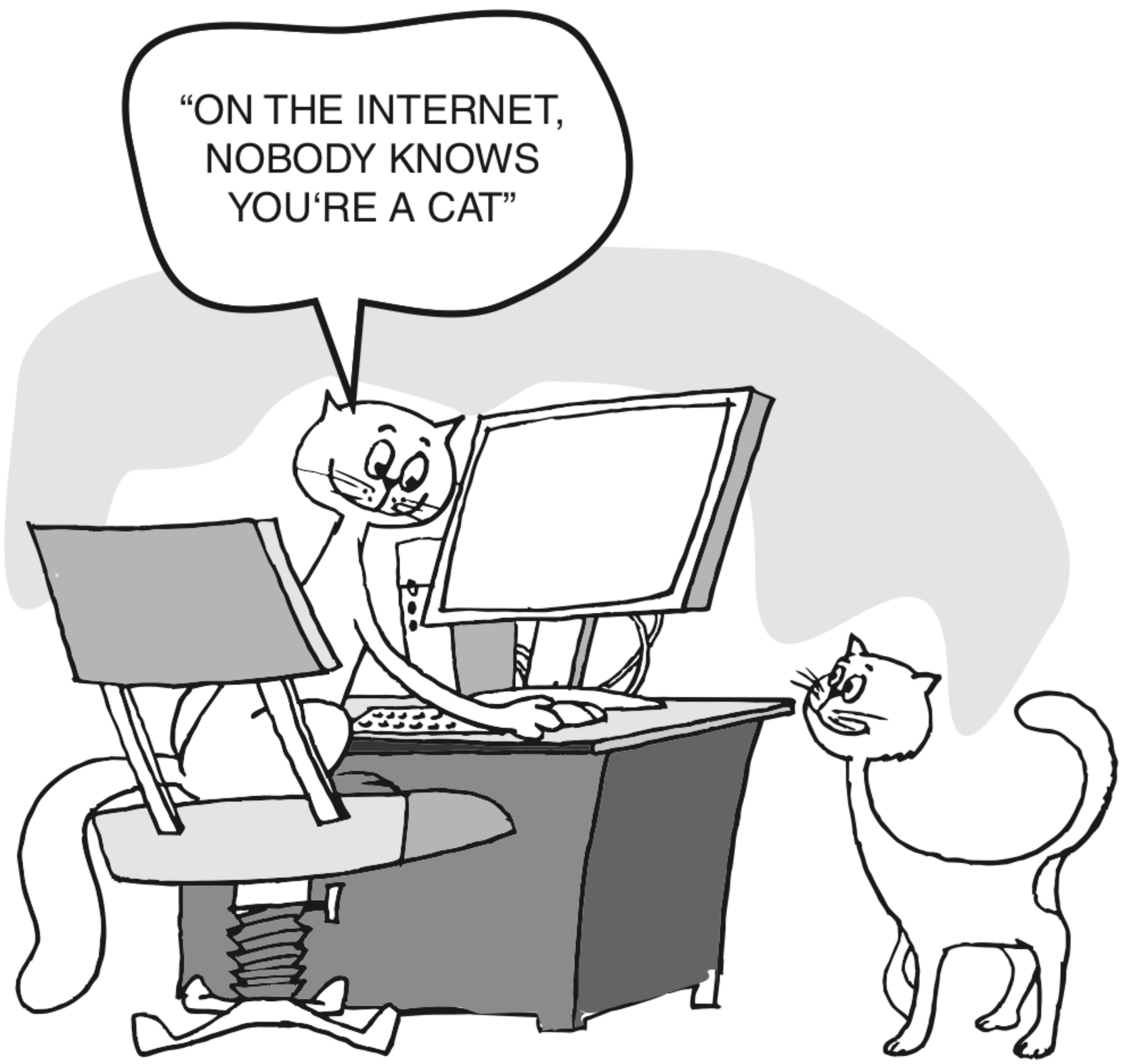


Figure 1.5 | Anonymity for Internet users.

2. It may amount to defamation to make an imputation concerning a company or an association or collection of persons as such.
3. An imputation in the form of an alternative or expressed ironically, may amount to defamation.
4. No imputation is said to harm a person's reputation unless that imputation directly or indirectly, in the estimation of others, lowers the moral or intellectual character of that person, or lowers the character of that person in respect of his caste or of his calling, or lowers the credit of that person, or causes it to be believed that the body of that person is in a loathsome state or in a state generally considered as disgraceful.

Libel is written defamation and *slander* is oral defamation. When determining whether or not defamation has taken place, the only issue to consider is whether a person of ordinary intelligence in society would believe that the words would indeed injure the person's reputation. Even if there is no (apparent) damage to a person's reputation, the person who made the allegations may still be held responsible for defamation.

The law on defamation attempts to create a workable balance between two equally important human rights: *The right to an unimpaired reputation* and *the right to freedom of expression*. In a cybersociety, both these interests are increasingly important. Protection of reputation is arguably even more important in a highly technological society, because one may not even encounter an individual or organization other than through the medium of the Internet. Some courts have held that the plaintiff must also have to show that the defamatory statements were unlawful and that it must not be for the defendant to justify his conduct by showing that the statements were in accordance with law. India's first case of cyberdefamation, at the Delhi Court, assumed jurisdiction over a matter where a corporate reputation was being defamed through E-Mails and passed an important ex-parte injunction. Further details on this case can be read at the link http://cyberlaws.net/cyberindia/defamation.htm (14 December 2009). Readers can also refer to the link http://en.wikipedia.org/wiki/Cyber_defamation_law (14 December 2009) for understanding cyberdefamation law.

1.5.4 Internet Time Theft

Such a theft occurs when an unauthorized person uses the Internet hours paid for by another person. Basically, Internet time theft comes under hacking because the person who gets access to someone else's ISP user ID and password, either by hacking or by gaining access to it by illegal means, uses it to access the Internet without the other person's knowledge. However, one can identify time theft if the Internet time has to be recharged often, even when one's own use of the Internet is not frequent. The issue of Internet time theft is related to the crimes conducted through "identity theft." In Chapter 11, there is a case described about theft of Internet time.

1.5.5 Salami Attack/Salami Technique

These attacks are used for committing financial crimes. The idea here is to make the alteration so insignificant that in a single case it would go completely unnoticed; for example a bank employee inserts a program, into the bank's servers, that deducts a small amount of money (say ₹ 2/- or a few cents in a month) from the account of every customer. No account holder will probably notice this unauthorized debit, but the bank employee will make a sizable amount every month. In Chapter 11, there are a number of examples, illustrations provided about use of Salami Technique in real life. Refer to Section 11.2 Real-Life Examples (Section 11.2.13 Example 13: Small "Shavings" for Big Gains! and Section 11.2.20 Example 20: The Petrol Pump Fraud).

1.5.6 Data Diddling

A data diddling attack involves altering raw data just before it is processed by a computer and then changing it back after the processing is completed. Electricity Boards in India have been victims to data diddling

programs inserted when private parties computerize their systems. In Chapter 11, there are a number of data diddling examples (refer to Section 11.2.6 Example 6: Doodle me Diddle!).

1.5.7 Forgery

Counterfeit currency notes, postage and revenue stamps, marksheets, etc. can be forged using sophisticated computers, printers and scanners. Outside many colleges there are miscreants soliciting the sale of fake marksheets or even degree certificates. These are made using computers and high quality scanners and printers. In fact, this is becoming a booming business involving large monetary amount given to student gangs in exchange for these bogus but authentic looking certificates.

1.5.8 Web Jacking

Web jacking occurs when someone forcefully takes control of a website (by cracking the password and later changing it). Thus, the first stage of this crime involves "password sniffing." The actual owner of the website does not have any more control over what appears on that website.

1.5.9 Newsgroup Spam/Crimes Emanating from Usenet Newsgroup

As explained earlier, this is one form of spamming. The word "Spam" was usually taken to mean excessive multiple posting (EMP). The advent of Google Groups, and its large Usenet archive, has made Usenet more attractive to spammers than ever. Spamming of Usenet newsgroups actually predates E-Mail Spam. The first widely recognized Usenet Spam titled *Global Alert for All: Jesus is Coming Soon* (though not the most famous) was posted on 18 January 1994 by Clarence L. Thomas IV, a sysadmin at Andrews University. It was a fundamentalist religious tract claiming that "this world's history is coming to a climax." The newsgroup posting Bot Serdar Argic also appeared in early 1994, posting tens of thousands of messages to various newsgroups, consisting of identical copies of a political screed relating to the Armenian Genocide.

1.5.10 Industrial Spying/Industrial Espionage

Spying is not limited to governments. Corporations, like governments, often spy on the enemy. The Internet and privately networked systems provide new and better opportunities for espionage. "Spies" can get information about product finances, research and development and marketing strategies, an activity known as "industrial spying." However, cyberspies rarely leave behind a trail. Industrial spying is not new; in fact it is as old as industries themselves. The use of the Internet to achieve this is probably as old as the Internet itself. Traditionally, this has been the reserved hunting field of a few hundreds of highly skilled hackers, contracted by high-profile companies or certain governments via the means of escrow organizations (it is said that they get several hundreds of thousands of dollars, depending on the "assignment").

With the growing public availability of Trojans and Spyware material (for Trojans and Spyware discussion, refer to Chapter 4 in the book and Chapter 3 of Ref. #1, Books, Further Reading), even low-skilled individuals are now inclined to generate high volume profit out of industrial spying. This is referred to as "Targeted Attacks" (which includes "Spear Phishing"). This aspect of *Industrial Spying* is the one to be addressed in the fight against cybercrime.

Organizations subject to online extortion tend to keep quiet about it to avoid negative publicity about them. Not surprisingly, this also applies very well to organizations that are victim of focused attacks aiming at stealing corporate data, Intellectual Property or whatever else that may yield a competitive advantage for a rival company.

One interesting case is the famous Israeli Trojan story,[9] where a software engineer in London created a Trojan Horse program specifically designed to extract critical data gathered from machines infected by his program. He had made a business out of selling his Trojan Horse program to companies in Israel, which would use it for industrial spying by planting it into competitors' networks. The methods used to inoculate the Trojan Horse were varied and sometimes quite inventive, ranging from simple E-Mail traps to the mailing of promotional CDs infected with the evil program! More about Trojan Horse is addressed in Chapter 2.

There are also the E-Mail worms automating similar "data exfiltration features." For example, the main characteristic of mass mailing worm deemed W32.Myfip.A[10] is to scan the hard drive of infected machines for all files with the following extensions: .pdf, .doc, .dwg, .sch, .pcb, .dwt, .dwf, .max, .mdb. Such files are uploaded on an FTP server owned by the cybercrooks, with the aim of stealing as much IP as possible wherever it can be and then selling it to people who are ready to pay for it. There are two distinct business models for cybercrime applied to industrial spying: *Selling Trojan-ware* and *Selling Stolen Intellectual Property.*

1.5.11 Hacking

Although the purposes of hacking are many, the main ones are as follows:

1. Greed;
2. power;
3. publicity;
4. revenge;
5. adventure;
6. desire to access forbidden information;
7. destructive mindset.

Every act committed toward breaking into a computer and/or network is hacking and it is an offense. Hackers write or use ready-made computer programs to attack the target computer. They possess the desire to destruct and they get enjoyment out of such destruction. Some hackers hack for personal monetary gains, such as stealing credit card information, transferring money from various bank accounts to their own account followed by withdrawal of money. They extort money from some corporate giant threatening him to publish the stolen information that is critical in nature. Government websites are hot on hackers' target lists and attacks on Government websites receive wide press coverage. For example, according to the story posted on December 2009, the NASA site was hacked via SQL Injection (see Ref. #22, Additional Useful Web References, Further Reading). SQL Injection is covered more in detail in Chapter 4. Examples of prominent websites hacked are shown in Figs. 1.6–1.10.

Hackers, crackers and phrackers[11] are some of the oft-heard terms. The original meaning of the word "hack" meaning an elegant, witty or inspired way of doing almost anything originated at MIT. The meaning has now changed to become something associated with the breaking into or harming of any kind of computer or telecommunications system. Some people claim that those who break into computer systems should ideally be called "crackers" and those targeting phones should be known as "phreaks" (see Chapter 17, Box 17.3 of Ref. #3, Books, Further Reading).

1.5.12 Online Frauds

Refer to Chapter 11, Section 11.7: Online Scams. There are a few major types of crimes under the category of hacking: Spoofing website and E-Mail security alerts, hoax mails about virus threats (refer to Chapter 4), lottery frauds and Spoofing. In Spoofing websites and E-Mail security threats, fraudsters create authentic

Figure 1.6 | Twitter site hacked.
Source: http://thenextweb.com/files/2009/12/Twitter-Hacked.png/ (14 July 2010).

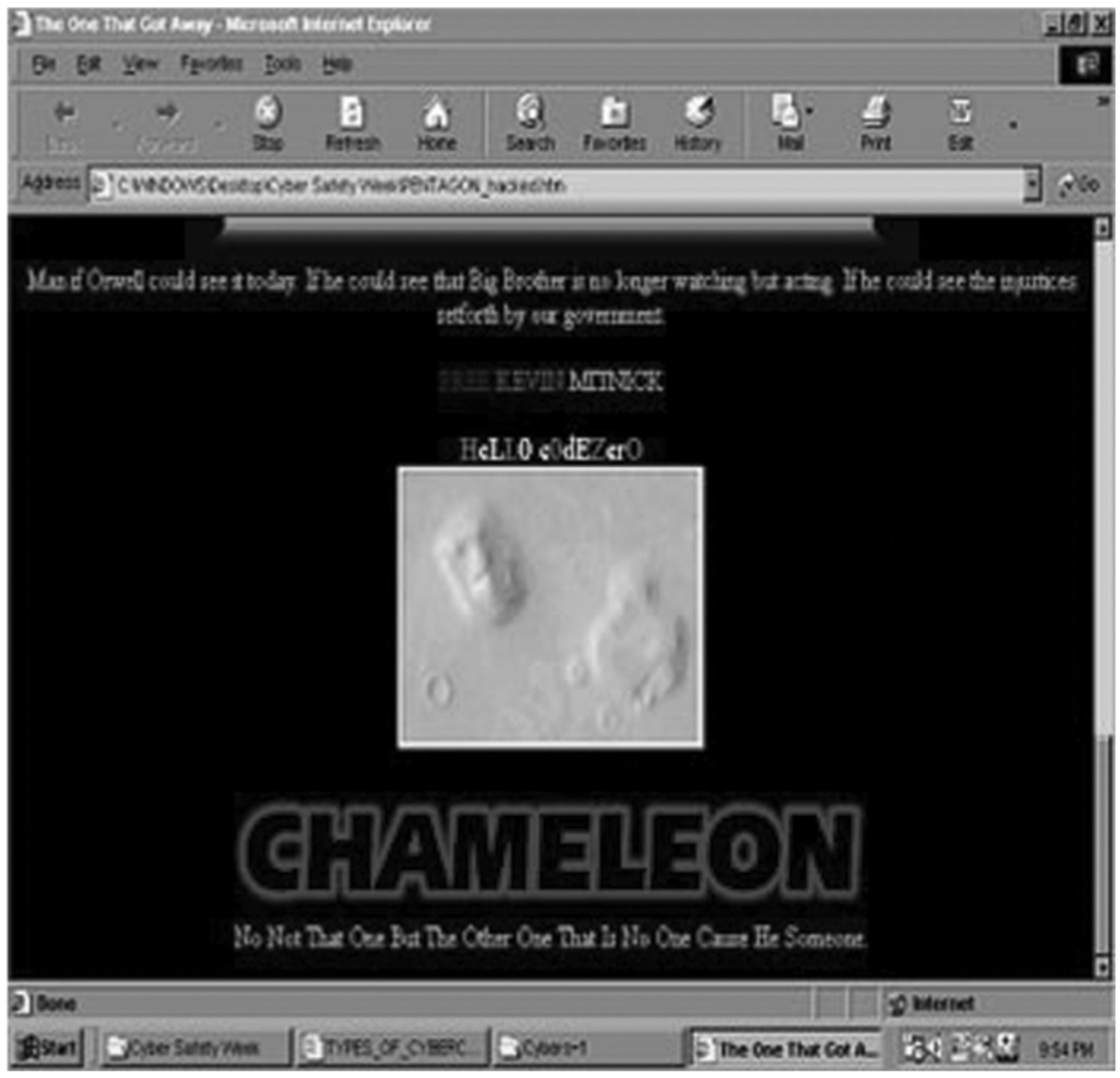


Figure 1.7 | Pentagon, the US site defaced.
Source: http://www.keylogger.org/news-world/hackers-attack-pentagon-1086.html

Box 1.4 The Story of a Hacked Website

Nadya Suleman (Nadya Denise Doud-Suleman Gutierrez), famously known as "Octomom" in the media, is an American woman who came to international attention when she gave birth to octuplets in January 2009. Nadya launched a website to solicit donations for her family. However, her site was immediately hacked by a group of vigilante mothers! Nadya's website originally featured photos of all eight octuplets, a thank you note from Suleman, images of children's toys and a large donation button for viewers to send money through. Suleman also provided an address where people can send items such as diapers and baby food formula. The site was hacked and brought down within hours. The original homepage was left defaced as seen in Fig. 1.8.

The site was tagged by the famous hacker group MOD, also known as the Mothers of Disappointment. The mysterious group has a history of attacking personal sites they disapprove of; so much for the "psychology" of hackers! Probably these "Mothers" were hungry for "recognition" (recall the classification of cybercriminals in Section 1.4).

Figure 1.8 | Octomom's defaced website.
Source: http://weeklyworldnews.com/headlines/6233/nadya-sulemans-website-hacked/

looking websites that are actually nothing but a spoof (see Chapter 5 for details of Spoofing). The purpose of these websites is to make the user enter personal information which is then used to access business and bank accounts. Fraudsters are increasingly turning to E-Mail to generate traffic to these websites. This kind of online fraud is common in banking and financial sector. Refer to Chapter 11, Section 11.4. There is a rise in the number of financial institutions' customers who receive such E-Mails which usually contain a link to a spoof website and mislead users to enter user ids and passwords on the pretence that security details can be updated or passwords changed. It is wise to be alert and careful about E-Mails containing an embedded link, with a request for you to enter secret details. It is strongly recommended not to input any sensitive information that might help criminals to gain access to sensitive information, such as bank account details, even if the page appears legitimate.

In virus hoax E-Mails, the warnings may be genuine, so there is always a dilemma whether to take them lightly or seriously. A wise action is to first confirm by visiting an antivirus site such as McAfee, Sophos or Symantec before taking any action, such as forwarding them to friends and colleagues.

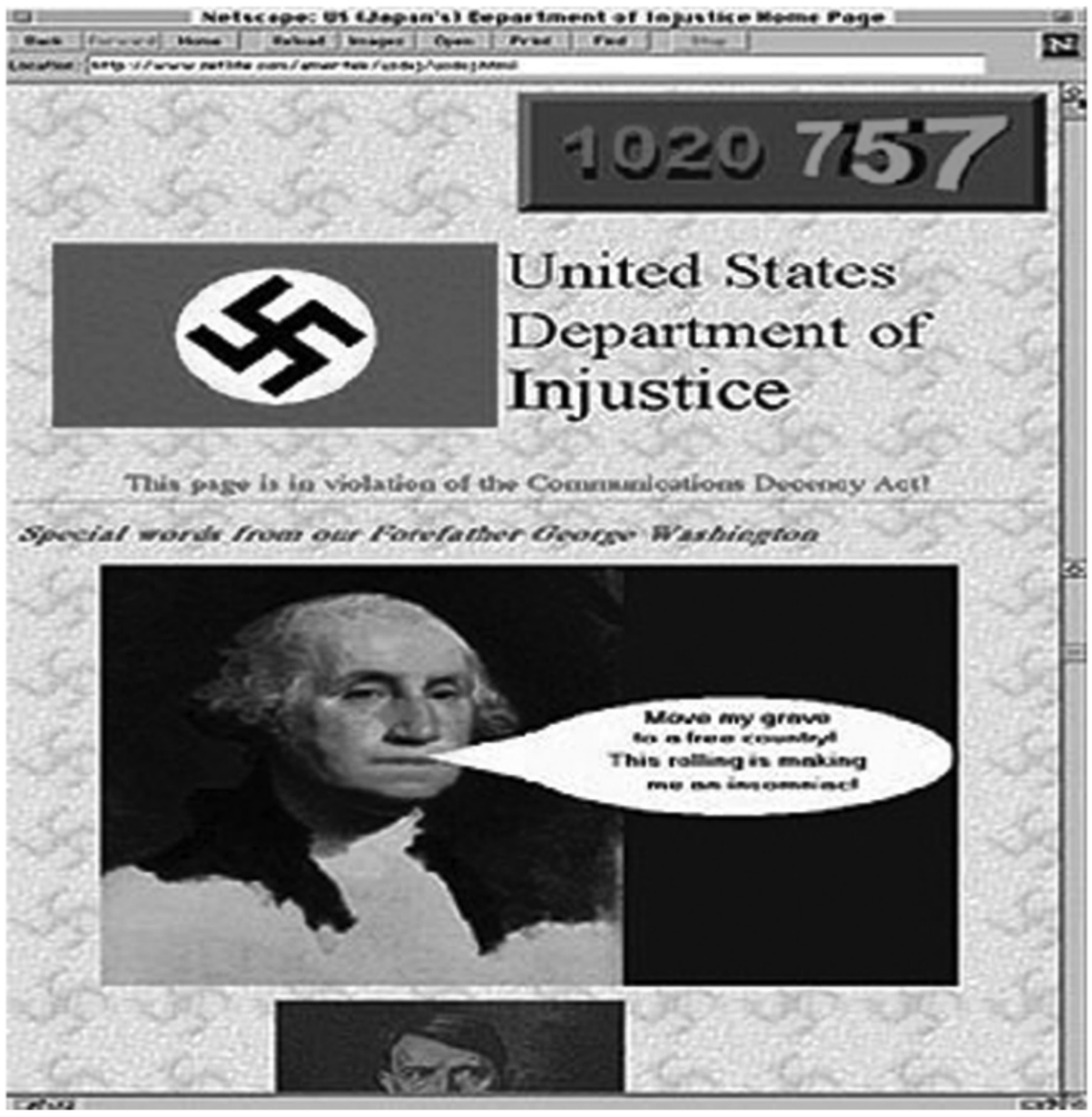


Figure 1.9 | Department of justice site defaced.
Source: http://www.technize.com/see-all-the-hacked-and-defaced-websites/

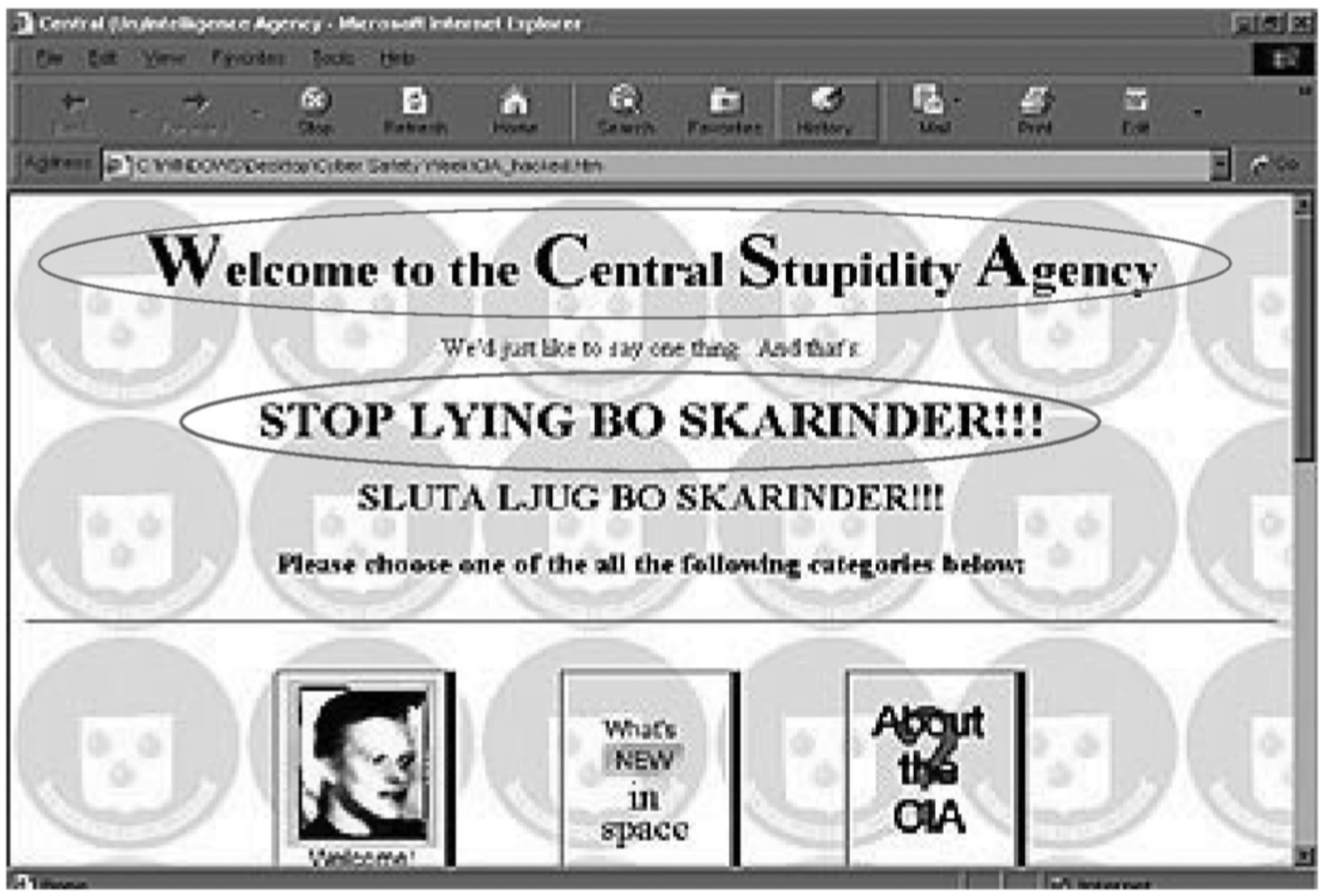


Figure 1.10 | CIA (Central Intelligence Agency), the US, website defaced.
Source: http://www.technize.com/see-all-the-hacked-and-defaced-websites/

Lottery frauds are typically letters or E-Mails that inform the recipient that he/she has won a prize in a lottery. To get the money, the recipient has to reply, after which another mail is received asking for bank details so that the money can be directly transferred. The E-Mail also asks for a processing fee/handling fee. Of course, the money is never transferred in this case; the processing fee is swindled and the banking details are used for other frauds and scams. Refer to Section 11.7.6, Chapter 11.

"Spoofing" means illegal intrusion, posing as a genuine user. A hacker logs-in to a computer illegally, using a different identity than his own. He is able to do this by having previously obtained the actual password. He creates a new identity by fooling the computer into thinking that the hacker is the genuine system operator and then hacker then takes control of the system. He can commit innumerable number of frauds using this false identity.

1.5.13 Pornographic Offenses

"Child pornography" means any visual depiction, including but not limited to the following:

1. Any photograph that can be considered obscene and/or unsuitable for the age of child viewer;
2. film, video, picture;
3. computer-generated image or picture of sexually explicit conduct where the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct.

Child pornography is considered an offense. Unfortunately, child pornography is a reality of the Internet. The Internet is being highly used by its abusers to reach and abuse children sexually, worldwide. In India too, the Internet has become a household commodity in the urban areas of the nation. Its explosion has made the children a viable victim to the cybercrime. As the broad-band connections get into the reach of more and more homes, larger child population will be using the Internet and therefore greater would be the chances of falling victim to the aggression of pedophiles. "Pedophiles" are people who physically or psychologically coerce minors to engage in sexual activities, which the minors would not consciously consent to. Here is how pedophiles operate:

Step 1: Pedophiles use a false identity to trap the children/teenagers (using "false identity" which in itself is another crime called "identity theft"). ID Theft is addressed in Chapter 5.
Step 2: They seek children/teens in the kids' areas on the services, such as the Teens BB, Games BB or chat areas where the children gather.
Step 3: They befriend children/teens.
Step 4: They extract personal information from the child/teen by winning his/her confidence.
Step 5: Pedophiles get E-Mail address of the child/teen and start making contacts on the victim's E-Mail address as well. Sometimes, these E-Mails contain sexually explicit language.
Step 6: They start sending pornographic images/text to the victim including child pornographic images in order to help child/teen shed his/her inhibitions so that a feeling is created in the mind of the victim that what is being fed to him is normal and that everybody does it.
Step 7: At the end of it, the pedophiles set up a meeting with the child/teen out of the house and then drag him/her into the net to further sexually assault him/her or to use him/her as a sex object.

This is the irony of the "digital world"; in physical world, parents know the face of dangers and they know how to avoid and face the problems by following simple rules and accordingly they advice their children to keep away from dangerous things and ways. However, it is possible, even in the modern times most parents may not know the basics of the Internet and the associated (hidden) dangers from the services offered over

the Internet. Hence most children may remain unprotected in the cyberworld. Pedophiles take advantage of this situation and lure the children, who are not advised by their parents or by their teachers about what is right/wrong for them while browsing the Internet. Legal remedies exist only to some extent; for example, Children's Online Privacy Protection Act or COPPA is a way of preventing online pornography. Interested readers are referred to COPPA sites.[12] Readers would like to note that Net Nanny and Cybersitter[13] are software, originally designed for parents concerned about their children's unrestricted access to the seamier side of the Internet, which can be used to block a user's access to websites containing "dangerous" or "offensive" material.

1.5.14 Software Piracy

This is a big challenge area indeed. (Readers may like to refer to Chapter 38 and other relevant pages of Ref. #3, Books, Further Reading.) Cybercrime investigation cell of India defines "software piracy" as *theft of software through the illegal copying of genuine programs or the counterfeiting and distribution of products intended to pass for the original.* There are many examples of software piracy: *end-user copying* – friends loaning disks to each other, or organizations under-reporting the number of software installations they have made, or organizations not tracking their software licenses; *hard disk loading with illicit means* – hard disk vendors load pirated software; *counterfeiting* – large-scale duplication and distribution of illegally copied software; *illegal downloads from the Internet* – by intrusion, by cracking serial numbers, etc. Beware that those who buy pirated software have a lot to lose: (a) getting untested software that may have been copied thousands of times over, (b) the software, if pirated, may potentially contain hard-drive-infecting viruses, (c) there is no technical support in the case of software failure, that is, lack of technical product support available to properly licensed users, (d) there is no warranty protection, (e) there is no legal right to use the product, etc.

Economic impact of software piracy is grave (see Fig. 1.11). According to the Fourth Annual BSA and IDC Global Software Piracy Study,[14] in Asia Pacific 55% of the software installed in 2006 on personal computers (PCs) was obtained illegally, while software losses due to software piracy amounted to US$ 11.6 billion. The Global Software Piracy Study mentioned covers all packaged software that runs on personal computers, including desktops, laptops and ultraportables. The study includes operating systems, systems software such as databases and security packages, business applications and consumer applications such as PC games, personal finance and reference software. Refer to Section 9.2.2, Chapter 9.

The BSA/IDC study of year 2006 did not include other types of software such as those which run on servers or mainframes or software sold as a service. It is shocking to know that 35% of the software installed in 2006 on PCs worldwide was obtained illegally, amounting to nearly $40 billion in global losses due to software piracy. Progress was seen in a number of emerging markets, most notably in China, where the piracy rate dropped 10 percentage points in 3 years, and in Russia, where piracy fell seven percentage points over 3 years. Figure 1.12 shows the regional scenario on piracy rate.

1.5.15 Computer Sabotage

The term "sabotage" has been mentioned many times in this chapter (Table 1.5, Section 1.2, Section 1.4 – Type II criminals, Table 1.6). The use of the Internet to hinder the normal functioning of a computer system through the introduction of worms, viruses (refer to Chapter 4) or logic bombs, is referred to as computer sabotage. It can be used to gain economic advantage over a competitor, to promote the illegal activities of terrorists or to steal data or programs for extortion purposes. Logic bombs are event-dependent programs created to do something only when a certain event (known as a trigger event) occurs. Some viruses may be termed as logic bombs because they lie dormant all through the

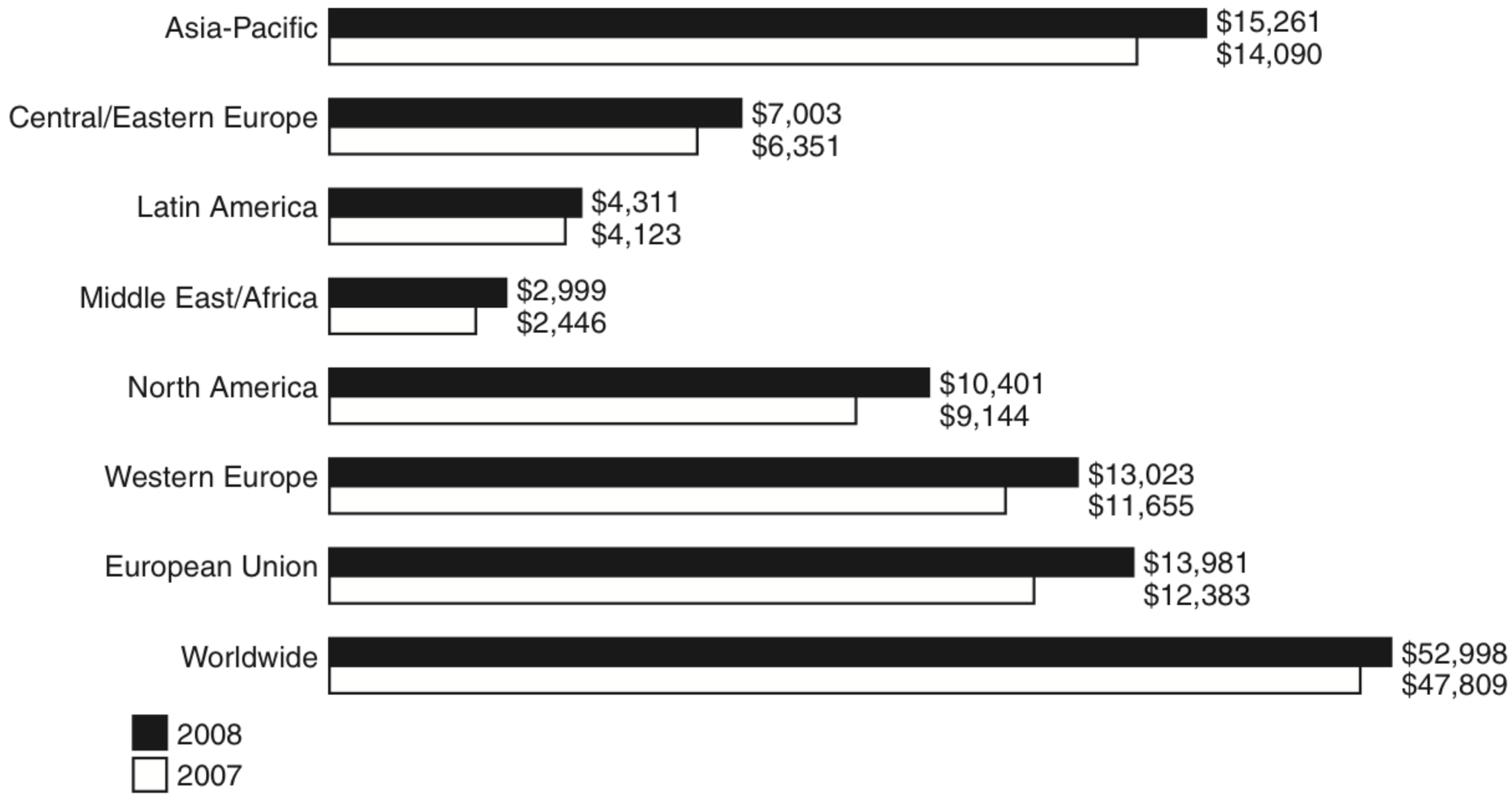


Figure 1.11 | Dollars lost (year 2008) due to (software) piracy – regional scenario.
Source: BSA-IDC Global 2008 Piracy Study released on May 2009 at the following link: http://global.bsa.org/globalpiracy2008/studies/globalpiracy2008.pdf (29 January 2010).

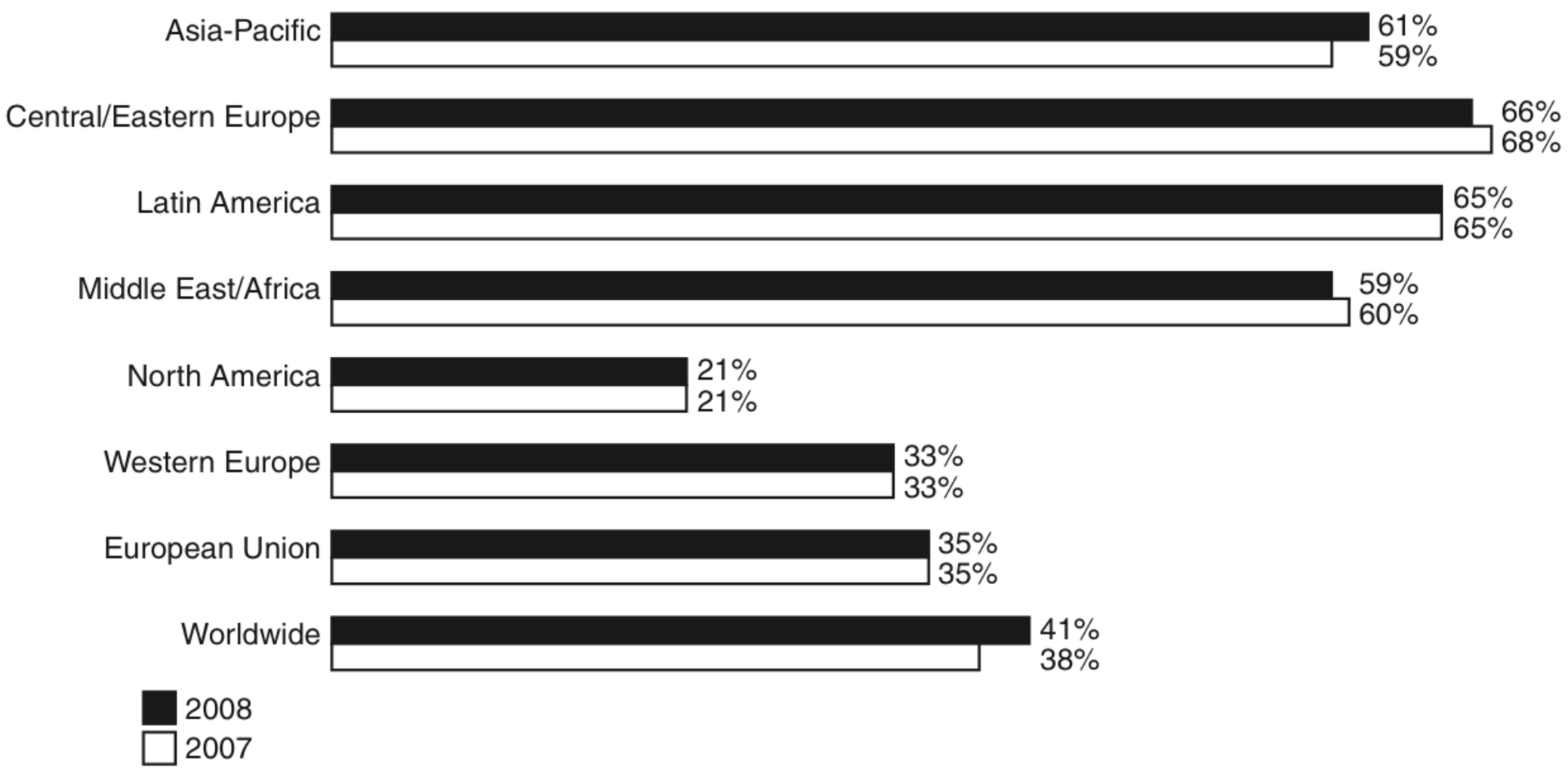


Figure 1.12 | Regional picture on piracy rate.
Source: BSA-IDC Global 2008 Piracy Study released on May 2009 at the following link: http://global.bsa.org/globalpiracy2008/studies/globalpiracy2008.pdf (29 January 2010).

year and become active only on a particular date (e.g., the Chernobyl virus and Y2K viruses[15]). Next, let us understand the term "mail bombs."

1.5.16 E-Mail Bombing/Mail Bombs

E-Mail bombing refers to sending a large number of E-Mails to the victim to crash victim's E-Mail account (in the case of an individual) or to make victim's mail servers crash (in the case of a company or an E-Mail service provider). Computer program can be written to instruct a computer to do such tasks on a repeated basis. In recent times, terrorism has hit the Internet in the form of mail bombings. By instructing a computer to repeatedly send E-Mail to a specified person's E-Mail address, the cybercriminal can overwhelm the recipient's personal account and potentially shut down entire systems. This may or may not be illegal, but it is certainly disruptive. Refer to Box 1.2, Tables 1.5 and 1.6 and Chapter 4 for DoS attacks.

1.5.17 Usenet Newsgroup as the Source of Cybercrimes

Usenet is a popular means of sharing and distributing information on the Web with respect to specific topic or subjects. Usenet is a mechanism that allows sharing information in a many-to-many manner. The newsgroups are spread across 30,000 different topics. In principle, it is possible to prevent the distribution of specific newsgroup. In reality, however, there is no technical method available for controlling the contents of any newsgroup. It is merely subject to self-regulation and net etiquette. It is feasible to block specific newsgroups, however, this cannot be considered as a definitive solution to illegal or harmful content. It is possible to put Usenet to following criminal use:

1. Distribution/sale of pornographic material;
2. distribution/sale of pirated software packages;
3. distribution of hacking software;
4. sale of stolen credit card numbers. Refer to Chapter 11, Section 11.4.2, Illustration 5;
5. sale of stolen data/stolen property.

1.5.18 Computer Network Intrusions

Computer Networks pose a problem by way of security threat because people can get into them from anywhere. The popular movie "War Games" illustrated an extreme but useful example of this. "Crackers" who are often misnamed "Hackers"[11] can break into computer systems from anywhere in the world and steal data, plant viruses, create backdoors, insert Trojan Horses or change user names and passwords. Network intrusions are illegal, but detection and enforcement are difficult. Current laws are limited and many intrusions go undetected.

The cracker can bypass existing password protection by creating a program to capture logon IDs and passwords. The practice of "strong password" is therefore important (password strength is explained in Chapter 4). Importance of passwords and password rules is explained in Chapter 11 (Network Security in Perspective) in Ref. #3, Books, Further Reading. In Ref. #3, Books, Chapter 35 (Auditing for Security) explains about password cracking tools in the context of vulnerability scanning and penetration testing. Refer to Ref. #3, Books, Chapter 17 (Security of Wireless Networks and Box 17.3 in particular) for crackers and hackers and Chapter 14 (Intrusion Detection for Securing Networks) for Trojans.

1.5.19 Password Sniffing

Password Sniffers are programs that monitor and record the name and password of network users as they login, jeopardizing security at a site. Whoever installs the Sniffer can then impersonate an authorized user

and login to access restricted documents. Laws are not yet set up to adequately prosecute a person for impersonating another person online. Laws designed to prevent unauthorized access to information may be effective in apprehending crackers using Sniffer programs. "Password cracking" and "password sniffing" are explained in Chapter 4.

1.5.20 Credit Card Frauds

Information security requirements for anyone handling credit cards have been increased dramatically recently. Millions of dollars may be lost annually by consumers who have credit card and calling card numbers stolen from online databases. Security measures are improving, and traditional methods of law enforcement seem to be sufficient for prosecuting the thieves of such information. Bulletin boards and other online services are frequent targets for hackers who want to access large databases of credit card information. Such attacks usually result in the implementation of stronger security systems. For more on credit card frauds see Chapter 3, Section 3.4 (Credit Card Frauds in Mobile and Wireless Computing Era) in Ref. #1, Books, Further Reading. Security of cardholder data has become one of the biggest issues facing the payment card industry. Payment Card Industry Data Security Standard (PCI-DSS) is a set of regulations developed jointly by the leading card schemes to prevent cardholder data theft and to help combat credit card fraud. We urge readers to visit the PCI-DSS-related URLs.[16] Refer to Chapter 11, Section 11.4.2.

1.5.21 Identity Theft

Identity theft is a fraud involving another person's identity for an illicit purpose. This occurs when a criminal uses someone else's identity for his/her own illegal purposes. Phishing and identity theft are related offenses (the topic is addressed in Chapter 5). Examples include fraudulently obtaining credit, stealing money from the victim's bank accounts, using the victim's credit card number (recall the discussion in the previous section

Box 1.5 Spam in Cyberworld

Basically, "Spam" is the abuse of electronic messaging systems to send unsolicited bulk messages indiscriminately. Although the most widely recognized form of Spam is E-Mail Spam, this term is applied to similar abuses in other media: instant messaging Spam, Usenet newsgroup Spam, web search engine Spam, Spam in blogs, wiki Spam, online classified ads Spam, mobile phone messaging Spam, Internet forum Spam, junk fax transmissions and file sharing network Spam. Spam is caused by flooding the Internet with many copies of the same message, in an attempt to force the message on people who would not otherwise choose to receive it. Often, this may result in the notorious DoS attack. Commercial advertising often happens to be the cause of Spam. Such advertisements are often for products of dubious reputation and fraud schemes meant to make people believe they can get rich overnight! Some Spam may also get generated through quasi-legal services. Spam hardly costs much to the sender; most of the costs are paid for by the recipient or the carriers rather than by the sender.

People who engage in the activity of electronic Spam are called spammers. Two main types of Spam are worth mentioning: "cancellable Usenet Spam" in which a single message is sent to several Usenet newsgroups and "E-Mail Spam" which targets individual users with direct mail messages. Often, spammers create E-Mail Spam lists by scanning Usenet postings, by stealing Internet mailing lists or searching the Web for addresses. Typically, it costs money to users if they receive E-Mail Spam. Any person with measured phone service can read or receive their mail. Spam does not cost much to people. Spam does, however, cost money to ISPs and to online service providers to transmit Spam. Unfortunately, subscribers end up paying these costs because the costs are transmitted directly to subscribers.

For further details, refer to Ref. #3 (Chapter 11, Denial-of-Service attacks, p. 177), Books, Further Reading.

about credit card frauds), establishing accounts with utility companies, renting an apartment or even filing bankruptcy using the victim's name. The cyberimpersonator can steal unlimited funds in the victim's name without the victim even knowing about it for months, sometimes even for years!

Thus far, we have provided an overview of various types of well-known cybercrimes. In most cybercrime forms, computers and/or other digital devices end up getting used as one or a combination of the following:

1. As the tool for committing cybercrime;
2. crime involving attack against the computer;
3. use for storing information related to cybercrime/information useful for committing cybercrime.

1.6 Cybercrime: The Legal Perspectives

Greater details on this are discussed in Chapter 6 and only a brief discussion is done in this section. Cybercrime poses a mammoth challenge. In the first comprehensive presentation of computer crime, *Computer Crime: Criminal Justice Resource Manual* (1979) (see Ref. #2, Additional Useful Web References, Further Reading), computer-related crime was defined in the broader meaning as: *any illegal act for which knowledge of computer technology is essential for a successful prosecution.* International legal aspects of computer crimes were studied in 1983. In that study, computer crime was consequently defined as: *encompasses any illegal act for which knowledge of computer technology is essential for its perpetration*.

Cybercrime, in a way, is the outcome of "globalization." However, globalization does not mean globalized welfare at all. Globalized information systems accommodate an increasing number of transnational offenses. The network context of cybercrime makes it one of the most globalized offenses of the present and the most modernized threats of the future. This problem can be resolved in two ways. One is to divide information systems into segments bordered by state boundaries (cross-border flow of information). The other is to incorporate the legal system into an integrated entity obliterating these state boundaries. Apparently, the first way is unrealistic. Although all ancient empires including Rome, Greece and Mongolia became historical remnants, and giant empires are not prevalent in current world, the partition of information systems cannot be an imagined practice. In a globally connected world, information systems become the unique empire without tangible territory.

1.7 Cybercrimes: An Indian Perspective

India has the fourth highest number of Internet users in the world. According to the statistics posted on the site (http://www.iamai.in/), there are 45 million Internet users in India, 37% of all Internet accesses happen from cybercafes and 57% of Indian Internet users are between 18 and 35 years. The population of educated youth is high in India. It is reported that compared to the year 2006, cybercrime under the Information Technology (IT) Act recorded a whopping 50% increase in the year 2007.[17] A point to note is that the majority of offenders were under 30 years. The maximum cybercrime cases, about 46%, were related to incidents of cyberpornography, followed by hacking. In over 60% of these cases, offenders were between 18 and 30 years, according to the "Crime in 2007" report of the National Crime Record Bureau (NCRB). Box 1.6 shows the Indian Statistics on cybercrimes. Also revisit Tables 1.1–1.4.

The Indian Government is doing its best to control cybercrimes. For example, Delhi Police have now trained 100 of its officers in handling cybercrime and placed them in its Economic Offences Wing. As at the time of writing this, the officers were trained for 6 weeks in computer hardware and software, computer networks comprising data communication networks, network protocols, wireless networks and network security.

Box 1.6 Cybercrimes: Indian Statistics

(A) Cybercrimes: Cases of Various Categories under ITA 2000

217 cases were registered under IT Act during the year 2007 as compared to 142 cases during the previous year (2006), thereby reporting an increase of 52.8% in 2007 over 2006. 22.3% cases (49 out of 217 cases) were reported from Maharashtra followed by Karnataka (40), Kerala (38) and Andhra Pradesh and Rajasthan (16 each).

45.6% (99 cases) of the total 217 cases registered under ITA 2000 were related to obscene publication/transmission in electronic form, known as cyberpornography. 86 persons were arrested for committing such offenses during 2007. There were 76 cases of hacking with computer system during the year wherein 48 persons were arrested. Out of the total (76) hacking cases, the cases relating to loss/damage of computer resource/utility under Section 66(1) of the IT Act were 39.5% (30 cases) whereas the cases related to hacking under Section 66(2) of IT Act were 60.5% (46 cases).

Maharashtra (19) and Kerala (4) registered maximum cases under Section 66(1) of the IT Act out of total 30 such cases at the National level. Out of the total 46 cases relating to hacking under Section 66(2), most of the cases (31) were reported from Karnataka followed by Kerala (7) and Andhra Pradesh (3). 29.9% of the 154 persons arrested in cases relating to ITA 2000 were from Maharashtra (46) followed by Karnataka and Madhya Pradesh (16 each). The age-wise profile of persons arrested in cybercrime cases under ITA 2000 showed that 63.0% of the offenders were in the age group 18–30 years (97 out of 154) and 29.9% of the offenders were in the age group 30–45 years (46 out of 154). Tamil Nadu reported two offenders whose ages were below 18 years.

India is said to be the "youth country" given the population age distribution. From the potential resources perspective, this is supposed to be a great advantage; assuming that these youths will get appropriate training to develop the required professional skills in them. However, from cybercrime perspective, this youth aspect does not seem good as revealed by cybercrime statistics in India. Crime head-wise and age-group-wise profile of the offenders arrested under ITA 2000 revealed that 55.8% (86 out of 154) of the offenders were arrested under "Obscene publication/transmission in electronic form" of which 70.9% (61 out of 86) were in the age group 18–30 years. 50% (24 out of 48) of the total persons arrested for "Hacking with Computer Systems" were in the age group of 18–30 years.

(B) Cybercrimes: Cases of Various Categories under IPC Section

A total of 339 cases were registered under IPC Sections during the year 2007 as compared to 311 such cases during 2006, thereby reporting an increase of 9.0%. Madhya Pradesh reported maximum number of such cases, nearly 46.6% of total cases (158 out of 339) followed by Andhra Pradesh 15.6% (53 cases) and Chhattisgarh 15.3% (52 cases). Majority of the crimes out of total 339 cases registered under IPC fall under two categories, viz., Forgery (217) and Criminal Breach of Trust or Fraud (73). Although such offenses fall under the traditional IPC crimes, these cases had the cyberovertones wherein computer, Internet or its enabled services were present in the crime and hence they were categorized as Cybercrimes under IPC. The cyberforgery (217 cases) accounted for 0.33% out of the 65,326 cases reported under cheating. The cyberfrauds (73) accounted for 0.47% of the total Criminal Breach of Trust cases (15,531).

The cyberforgery cases were the highest in Madhya Pradesh (133) followed by Chhattisgarh (26) and Andhra Pradesh (22). The cases of cyberfraud were highest in Madhya Pradesh (20) followed by Punjab (17) and Andhra Pradesh (15). A total of 429 persons were arrested in the country for Cybercrimes under IPC during 2007. 61.5% offenders (264) of these were taken into custody for offenses under "Cyberforgery," 19.8% (85) for "Criminal Breach of Trust/Fraud" and 11.4% (49) for "Counterfeiting Currency/Stamps."

States such as Madhya Pradesh (166), Andhra Pradesh (83), Chhattisgarh (82) and Punjab (69) have reported higher arrests for cybercrimes registered under IPC. The age-group-wise profile of the arrested persons showed that 55.2% (237 of 429) were in the age group of 30–45 years and 29.4% (126 of 429) of the offenders were in the age group of 18–30 years. Only four offenders from Chhattisgarh were below 18 years of age. Crime head-wise and age-wise profile of the offenders arrested under Cybercrimes (IPC) offenders involved in forgery cases were more in the age group of 30–45 (54.9%, 145

Box 1.6 Cybercrimes: . . . (*Continued*)

of 264). 57.6% of the persons arrested under Criminal Breach of Trust/Cyberfraud offenses were in the age group 30–45 years (49 out of 85).

(C) Incidence of Cybercrimes in Cities

17 out of 35 mega cities did not report any case of cybercrime (neither under the IT Act nor under IPC Sections) during the year 2007. A total of 17 mega cities have reported 118 cases under IT Act and 7 mega cities reported 180 cases under various sections of IPC. There was an increase of 32.6% (from 89 cases in 2006 to 118 cases in 2007) in cases under IT Act as compared to previous year (2006), and an increase of 26.8% (from 142 cases in 2006 to 180 cases in 2007) of cases registered under various sections of IPC. Bengaluru (40), Pune (14) and Delhi (10) have reported high incidence of cases (64 out of 118 cases) registered under IT Act, accounting for more than half of the cases (54.2%) reported under the Act. Bhopal has reported the highest incidence (158 out of 180 cases) of cases reported under IPC sections accounting for 87.8%.

1.8 Cybercrime and the Indian ITA 2000

In India, the ITA 2000 was enacted after the United Nation General Assembly Resolution A/RES/51/162 in January 30, 1997 by adopting the Model Law on Electronic Commerce adopted by the United Nations Commission on International Trade Law. This was the first step toward the Law relating to E-Commerce at international level to regulate an alternative form of commerce and to give legal status in the area of E-Commerce. It was enacted taking into consideration UNICITRAL model of Law on Electronic Commerce (1996).[18]

1.8.1 Hacking and the Indian Law(s)

Cybercrimes are punishable under two categories: the ITA 2000 and the IPC (see Tables 1.1 and 1.2). A total of 207 cases of cybercrime were registered under the IT Act in 2007 compared to 142 cases registered in 2006. Under the IPC too, 339 cases were recorded in 2007 compared to 311 cases in 2006. There are some noteworthy provisions under the ITA 2000, which is said to be undergoing key changes very soon (as at the time of writing this, Table 1.7).

Table 1.7 | The key provisions under the Indian ITA 2000 (before the amendment)

Section Ref. and Title	*Chapter of the Act and Title*	*Crime*	*Punishment*
Sec. 43 (Penalty for damage to computer, computer system, etc.)	CHAPTER IX Penalties and Adjudication	Damage to computer system, etc.	Compensation for ₹ 1 crore (₹ 10,000,000).
Sec. 66 (Hacking with computer system)	CHAPTER XI Offences	Hacking (with intent or knowledge).	Fine of ₹ 2 lakhs (₹ 200,000) and imprisonment for 3 years.
Sec. 67 (Publishing of information which is obscene in electronic form)	CHAPTER XI Offences	Publication of obscene material in electronic form.	Fine of ₹ 1 lakh (₹ 100,000), imprisonment of 5 years and double conviction on second offence.

(*Continued*)

Table 1.7 | (*Continued*)

Section Ref. and Title	*Chapter of the Act and Title*	*Crime*	*Punishment*
Sec. 68 (Power of controller to give directions)	CHAPTER XI Offences	Not complying with directions of controller.	Fine up to ₹ 2 lakhs (₹ 200,000) and imprisonment of 3 years.
Sec. 70 (Protected system)	CHAPTER XI Offences	Attempting or securing access to computer of another person without his/her knowledge.	Imprisonment up to 10 years.
Sec. 72 (Penalty for breach of confidentiality and privacy)	CHAPTER XI Offences	Attempting or securing access to computer for breaking confidentiality of the information of computer.	Fine up to ₹ 1 lakh (₹ 100,000) and imprisonment up to 2 years.
Sec. 73 (Penalty for publishing Digital Signature Certificate false in certain particulars)	CHAPTER XI Offences	Publishing false digital signatures, false in certain particulars.	Fine of ₹ 1 lakh (₹ 100,000) or imprisonment of 2 years or both.
Sec. 74 (Publication for fraudulent purpose)	CHAPTER XI Offences	Publication of Digital Signatures for fraudulent purpose.	Imprisonment for the term of 2 years and fine of ₹ 1 lakh (₹ 100,000).

Source: Information Technology Act 2000, Act no. 21, accessible at the URL: http://www.commonlii.org/in/legis/num_act/ita2000258/ (22 February 2000).

Box 1.7 Hacking and the ITA 2008

The number of Offenses to be monitored has increased. According to cyberlaw experts, "Any criminal activity that uses a computer either as an instrumentality, target or a means for perpetuating further crimes comes within the ambit of cybercrime." Cases of Spam, hacking, cyberstalking and E-Mail fraud are rampant and, although cybercrimes cells have been set up in major cities, the problem is that most cases remain unreported due to a lack of awareness. In a milieu like this, there are a number of pertinent questions in the minds of a commoner: When can consumers approach a cybercrime cell? What should the victims do? How does one maintain security online?

Any and every incident of cybercrime involving a computer or electronic network can be reported to a police station, irrespective of whether it maintains a separate cell or not. CHAPTER XI of the original ITA 2000 lists a number of activities that may be taken to constitute cybercrimes. This includes tampering with computer source code, hacking, publishing or transmitting any information in electronic form that is lascivious, securing access to a protected system, and breach of confidentiality and privacy. In the original ITA 2000, the following is stated under CHAPTER XI (Offences):

1. Whoever with the intent to cause or knowing that he is likely to cause wrongful loss or damage to the public or any person destroys or deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means, commits hack.
2. Whoever commits hacking shall be punished with imprisonment up to 3 years, or with fine which may extend up to ₹ 2 lakhs (₹ 200,000), or with both.

Box 1.7 Hacking . . . (*Continued*)

In the amendment to the IT Act 2000, now known as the ITA 2008, several offenses have been added to the Act. The amendments have now revealed a whole bundle of surprises which will make the cybercrime police jump. Existing Sections 66 and 67 (in the original ITA 2000) on hacking and obscene material have been updated by dividing them into more crime-specific subsections, thereby making cybercrimes punishable.

In Section 66, hacking as a term has been removed. This section has now been expanded to include Sections 66A (offensive messages), 66B (receiving stolen computer), 66C (identity theft), 66D (impersonation), 66E (voyeurism) and 66F (cyberterrorism). Section 66F is a new section of the ITA 2008 (recent amendments to the Indian ITA 2000). It covers "Cyberterrorism" and makes it punishable with imprisonment up to life term. This may cover hacking, DoS attacks, Port Scanning, spreading viruses, etc., if it can be linked to the object of terrorizing people. Conspiracy is also covered under the section. The offense is not bailable or compoundable. Refer to Chapter 4 to know more on computer viruses.

1.9 A Global Perspective on Cybercrimes

Cybercrime definitions were provided in Section 1.2. As mentioned there, statute and treaty law both refer to cybercrime. In Australia, cybercrime has a narrow statutory meaning as used in the *Cyber Crime Act* 2001, which details offenses against computer data and systems. However, a broad meaning is given to cybercrime at an international level. In the Council of Europe's (CoE's) *Cyber Crime Treaty*, cybercrime is used as an umbrella term to refer to an array of criminal activity including offenses against computer data and systems, computer-related offenses, content offenses and copyright offenses. This wide definition of cybercrime overlaps in part with general offense categories that need not be Information & Communication Technology (ICT)-dependent, such as white-collar crime and economic crime. Figure 1.13 shows countries taking actions against Spam. Although this status is from the International Telecommunication Union (ITU) survey conducted in 2005, we get an idea about the global perspective. The status on E-Mail Spam legislation by country is available at the site http://en.wikipedia.org/wiki/E-mail_spam_legislation_by_country (29 January 2010). ITU activities on countering Spam can be read by visiting the link www.itu.int/spam (8 May 2010).

The Spam legislation scenario mentions "none" about India as far as E-Mail legislation in India is concerned. The legislation refers to India as a "loose" legislation, although there is a mention in Section 67 of Indian ITA 2000. See Table 1.7.

About 30 countries have enacted some form of anti-Spam legislation (see Fig. 1.13). There are also technical solutions by ISPs and end-users. However, in spite of this, so far there has been no significant impact on the volume of Spam with spammers sending hundreds of millions of messages per day. The growing phenomenon is the use of Spam to support fraudulent and criminal activities – including attempts to capture financial information (e.g., account numbers and passwords) by masquerading messages as originating from trusted companies ("brand-spoofing" or "Phishing") – and as a vehicle to spread viruses and worms. On mobile networks, a peculiar problem is that of sending of bulk unsolicited text messages aimed at generating traffic to premium-rate numbers. As there are no national "boundaries" to such crimes under cybercrime realm, it requires international cooperation between those who seek to enforce anti-Spam laws.

Thus, one can see that there is a lot to do toward building confidence and security in the use of ICTs and moving toward international cooperation agenda. This is because in the 21st century, there is a growing dependency on ICTs that span the globe. There was a rapid growth in ICTs and dependencies that led to shift in perception of cybersecurity threats in mid-1990s. The linkage of cybersecurity and critical infrastructure protection has become a big issue as a number of countries have began assessment of threats,

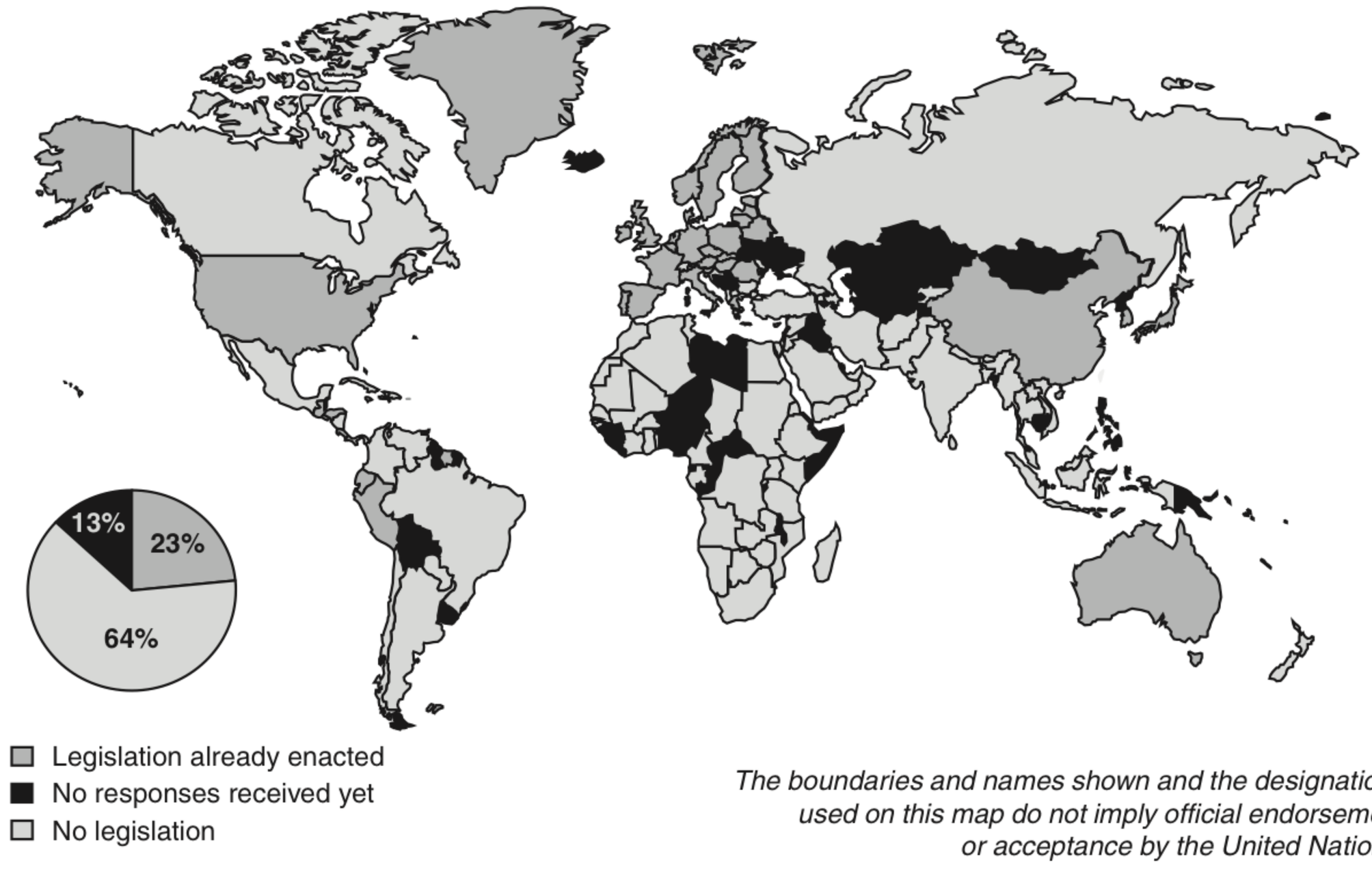


Figure 1.13 Worldwide picture on anti-Spam legislation.
Source: From the Presentation by Cristina Bueti, Programme Coordinator International Telecommunication Union, at the EU Spam Symposium, June 2006 at Maastricht, Holland – presentation can be accessed at the URL: http://spamsymposium.eu/files/Cristina%20Bueti.ppt#1 (8 May 2010).

vulnerabilities and started exploring mechanisms to redress them. Recently, there have been a number of significant developments such as

1. August 4, 2006 Announcement: The US Senate ratifies CoE Convention on Cyber Crime. The convention targets hackers, those spreading destructive computer viruses (refer to Chapter 4), those using the Internet for the sexual exploitation of children or the distribution of racist material, and terrorists attempting to attack infrastructure facilities or financial institutions. The Convention is in full accord with all the US constitutional protections, such as free speech and other civil liberties, and will require no change to the US laws.
2. In August 18, 2006, there was a news article published "ISPs Wary About 'Drastic Obligations' on Web Site Blocking." European Union (EU) officials want to debar suspicious websites as part of a 6-point plan to boost joint antiterrorism activities. They want to block websites that incite terrorist action. Once again it is underlined that monitoring calls, Internet and E-Mail traffic for law enforcement purposes is a task vested in the government, which must reimburse carriers and providers for retaining the data.
3. CoE Cyber Crime Convention (1997–2001) was the first international treaty seeking to address Internet crimes by harmonizing national laws, improving investigative techniques and increasing cooperation among nations.[19] More than 40 countries have ratified the Convention to date.

1.10 Cybercrime Era: Survival Mantra for the Netizens

The term "Netizen" was coined by Michael Hauben. Quite simply, "Netizens" are the Internet users. Therefore, by corollary, "Netizen" is someone who spends considerable time online and also has a considerable presence online (through websites about the person, through his/her active blog contribution and/or also his/her participation in the online chat rooms). The 5P Netizen mantra for online security is: (a) Precaution, (b) prevention, (c) Protection, (d) Preservation and (e) Perseverance. For ensuring cybersafety, the motto for the "Netizen" should be "Stranger is Danger!" If you protect your customer's data, your employee's privacy and your own company, then you are doing your job in the grander scheme of things to regulate and enforce rules on the Net through our community. [Refer to Chapters 29–31, Ref. #3, Books, Further Reading for a detailed discussion on the topic of "privacy" and its impact on business as well as technological impact on privacy (RFID, Software Agents, Smart Cards, etc.).] Refer to Part I of Appendix D (in CD).

NASSCOM urges that cybercrime awareness is important, and any matter should be reported at once. This is the reason they have established cyberlabs across major cities in India (Ref. #6, Additional Useful Web References, Further Reading). More importantly, users must try and save any electronic information trail on their computers. That is all one can do until laws become more stringent or technology more advanced. Refer to Appendices U and V (in CD).

Some agencies have been advocating for the need to address protection of the Rights of Netizens. There are agencies that are trying to provide guidance to innocent victims of cybercrimes. However, these NGO-like efforts cannot provide complete support to the victims of cybercrimes and are unable to get the necessary support from the Police. There are also a few incidents where Police have pursued false cases on innocent IT professionals. The need for a statutorily empowered agency to protect abuse of ITA 2000 in India was, therefore, a felt need for quite some time. Chapter 6 addresses further details on the Indian ITA 2000 and its subsequent amendments in the year 2008.

1.11 Concluding Remarks and Way Forward to Further Chapters

This chapter sets the context for the rest of the book; in that sense, this is a "curtain raiser" chapter. Having provided a broad overview about cybercrime, in the subsequent chapters reader will be taken through other key aspects of cybercrime: how the crimes are planned, the tools and methods used for launching the attacks, light on legal aspects of cybercrime, cyberforensics, social as well as psychological and ethical dimensions of cybercrime, organizational implications, career implications, etc. Chapter 11 has extensive illustrations on cybercrime. For the reasons of confidentiality and protection of individual privacy, the names and other details are masked; however the scenarios are real. If there happens to exist any individual by the name mentioned, living or deceased, then it would be a pure coincidence. A key message, as we end this chapter, is for the ethical hacking community; while some people argue that there should be no such term as "ethical hacking" because there cannot be anything ethical about hacking, the need for and availability of professional certifications such as "Certified Ethical Hacking" is purely for investigative nature. Even such individuals who work on commercial terms when invited to hack systems for vulnerability assessment, should remember that their job is highly onerous and that they should bear in mind their ethical responsibility all the time. These aspects are explained in Chapter 35, Ref. #3, Books, Further Reading.

Summary

Cyberspace is one of the great legal frontiers of our time. Cybercrime is a term which is used to describe the act in which computers and networks are targeted for criminal activity. Such crimes have emerged as a new class of crimes, rapidly increasing due to extensive use of the Internet and IT-enabled services. We learnt in this chapter that there are many types of computer-related crimes. Cybercrimes range from tampering with computer documents, hacking and cyberpornography to false electronic evidence, unauthorized access to protected computer documents and breach of confidentiality. Within India and worldwide, there has been a phenomenal rise in the incidents of cybercrime. The issue of cybercrime continues to grow as a controversy for several reasons. We need laws that protect us from computer crimes, but we also need laws that are not so controlling that they compromise our civil liberties and constitutional rights.

Review Questions

1. What is cybercrime? How do you define it?
2. How do we classify cybercrimes? Explain each one briefly.
3. What are the different types of cybercriminals?
4. Is there a difference between "cybercrime" and "cyberfraud"? Explain.
5. How do viruses get disseminated? Explain with diagrams.
6. Write a short note on "Indian Legal Perspective on Cybercrime." You may like to augment your note using your own research, in addition to the material presented in this chapter.
7. How do you think cybercrime has relevance in the extended enterprise context? Explain.
8. Explain in your own words what you understand about the global cooperation required in fighting against cybercrime.

References

[1] *Information Security Glossary* can be visited at: http://www.yourwindow.to/information-security/gl_cybercrime.htm (14 March 2009).

[2] http://qanda.encyclopedia.com/question/cybernetics-related-84610.html (2 February 2009).

[3] http://www.pangaro.com/published/cyber-macmillan.html (26 February 2009).

[4] http://www.catunesco.upc.es/ads/beer.pdf (26 February 2009).

[5] http://www.gwu.edu/~asc/cyber_definition.html (26 February 2009).

[6] http://en.wikipedia.org/wiki/Cybernetics (20 February 2009).

[7] Site for *Information Technology Act 2000 Amendment* can be visited at: http://cybercrime.planetindia.net/new-cyber-security-infrastructure.htm (14 March 2009).

[8] 2008 CSI Computer Crime and Security Survey can be assessed at: http://i.cmpnet.com/v2.gocsi.com/pdf/CSIsurvey2008.pdf (15 March 2009).

[9] Israeli Trojan Horse scandal can be visited at: http://www.msnbc.msn.com/id/8064757/ (18 March 2009).

[10] To understand the technical details involved inW32.Myfip.A, visit the technical document available at: http://www.symantec.com/avcenter/reference/when.malware.meets.rootkits.pdf (12 February 2009).

[11] Loza, B. http://www.safepatrolsolutions.com/papers/Crackers.pdf (1 February 2010).