10 Cybercrime and Cyberterrorism: Social, Political, Ethical and Psychological Dimensions

Learning Objectives

After reading this chapter, you will able to:

- Understand "ethics," "computer ethics" and will appreciate their importance in cyberspace.
- Note the relation between "ethics" and "morality."
- Learn about ethical hackers.
- Know about different forms of "intellectual property."
- Understand the "generations" of hackers.
- Know what young generation thinks about hacking skills.
- Gain insight into sociological aspects of computer criminals.
- Learn about "Information Warfare" – the emerging threat to digital economy.

10.1 Introduction

In common parlance, the word "hacker" is used to mean someone who illegally breaks into a computer or network or writes a Malicious Code (worm or virus).

According to some people, "hacking" is a media-centric abuse of the word and they feel that the term "hacking" does not represent any illegal activities. For the purpose of this chapter, we shall accept this more limited definition. If "they" are cybercriminals (hackers included), "we" refers to network security professionals and network administrators acting on behalf of clients and employers in the defense of IT infrastructure and data. Often, we hear that a certain hacker breaks into a system and steals credit card numbers, releases a destructive worm or maybe defaces a website. What do we think about his/her actions? Are the actions of hackers ethical or unethical? Most of us would agree that such actions indicate unethical behavior. What about us though? How should our actions be viewed when we, in defense of our clients' networks or our own networks, engage in activities similar to those of hacker?

There are many sophisticated terms to describe hackers and cybercriminals. For example, there are terms such as "novice" (newbies/script kiddies), "cyberpunks" (refer to Box 1.1 of Chapter 1), "insiders" (refer to Fig. 9.2, Sections 9.1.1 and 9.1.2 in Chapter 9), "coders," "cyberterrorists." Terms such as "political activists" or "hacktivist" are also used perhaps for a glorious justification!. Modern day cybercriminals work like "Pros."

They use sophisticated methods and tools for planning cyberattacks and to exploit security weaknesses (see Chapters 2 and 4). It does not take too many cybercriminals to cause havoc in IT systems than it takes criminals in the real world to upset society. "Victimless crimes" are on the rise – for example, the subverting and repurposing of software poses huge problems for law enforcement agencies; particularly when "crimes" in cyberspace are taken less seriously. Many scenarios and case illustrations provided in Chapter 11 (in CD) bring forth the dangers in cyberspace. A number of questions come to our minds. Why do people hack? What drives people to steal information that does not belong to them? What is wrong with certain segment of people that causes them to bring harm to others. Why individuals become involved in delinquent behavior? How do they justify the behavior they engage in?

Modern day cybercriminals work like "Pros." They use methods of planning cyberattacks and tools used by hackers to exploit security weaknesses.

Do we have answers to these questions? Can we ever comprehend the motives behind cybercrimes? In Section 1.4 of Chapter 1, we mentioned about possible motives and categories of cybercriminals. Ethics is the branch of philosophy that deals with what is considered to be right and wrong. Computer ethics is important considering its ramifications and impacts on the related domains – see Fig. 10.1.

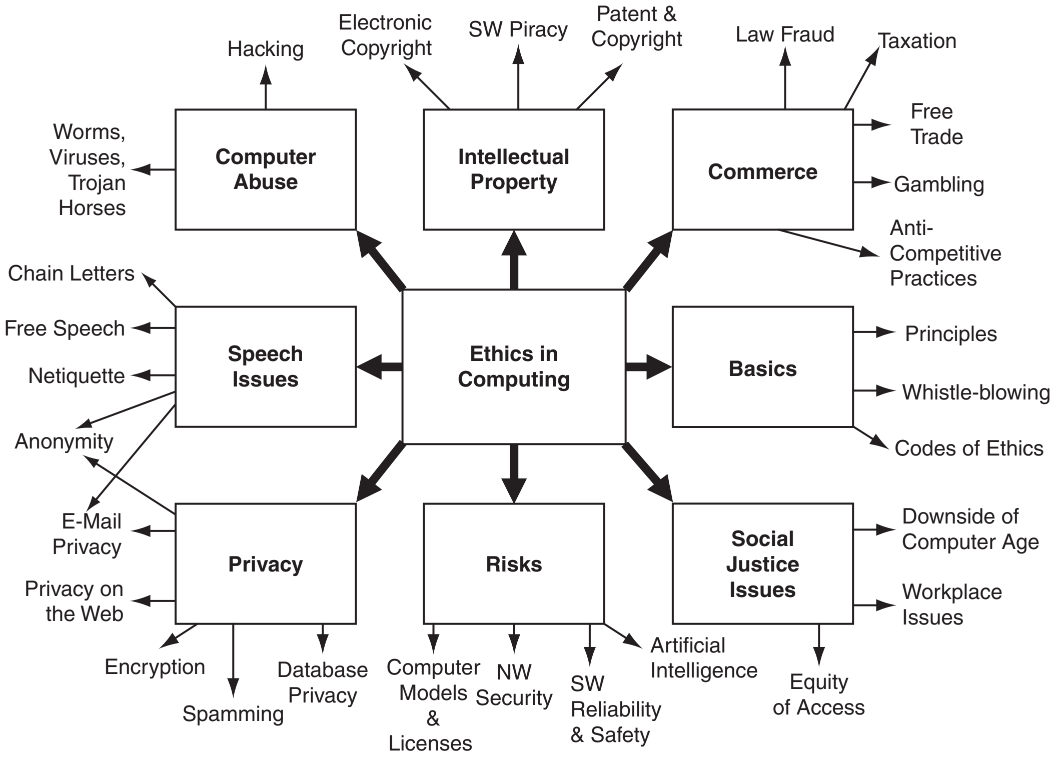

Figure 10.1 Ethics in computing.

Ethics and morality both have a relation with human behavior and attitude. Attempting to change people's behaviors or attitudes seems a challenge; it is an ethical minefield! A persuasive communications paradigm has multiple roles and many people are involved – salespersons, political activists, solicitors, etc. to name a few. We may not believe that the persuader has our best interests in mind. As is the case with all new technologies, ethical considerations trail behind technological capabilities. We may feel under our own pressure or social pressure to take a particular action. This is because our lives are now hopelessly tangled with Information and Communication Technology (ICT) and inter-related agencies. All are connected through the network where "information" is the common "glue" that gets smoothly exchanged with interested parties with the help of millions of computer networks and servers around the world. The very concept of anonymity has come in only recently. In the medieval society there was no notion of personal privacy; everyone knew everything about everyone.

"Privacy" is the right to be left alone and the right to be free of unreasonable personal intrusions.

Two rules have been followed fairly closely in court decisions: (a) the right of privacy is not absolute. Privacy must be balanced against the needs of society. (b) The public's right to know is superior to the individual's right of privacy. Privacy implications of technology are discussed in Ref. #3, Books, Further Reading. The scenario described below is with reference to the use of RFID (radio frequency identification) and its privacy implications explained in the quoted book at the end of this chapter. The scenario described next is a hypothetical example meant only to demonstrate the tension between ethical considerations and technology.

Consider this scenario – you are living in a technologically advanced country. Suppose one afternoon you go out to buy diesel/fuel for a lawn mower and a popular variety of garden fertilizer and you visit two shops to do this. When you return home you find that the cops are waiting for you. What could you have possibly done wrong in getting those products for your personal use? It could have happened that both products had embedded Radio Frequency Identification (RFID) tags and together, the two products you bought alerted the law enforcement agency. Maybe you have keen interest in gardening; but you could be a terrorist involved in making a bomb or you could be hobby bomb-maker! How is that possible? Well, out of curiosity you search the Net for the words "diesel" and "fertilizer," bringing up websites with full instructions on bomb-making. Spyware could track this request, leading to cop's attention. Figure 10.1 shows the multiple dimensions of ethics in the context of cybercrimes (for its broad definition refer to Chapter 1). As you can see in Fig. 10.1, there are ethical issues associated with intellectual property (IP). Different types of IPs are presented in the next section. We need to understand how the IP gets impacted when cybercriminals do their travails of stealing other people's IP through various illicit means. We as the netizens (citizens who have a long dwelling and dependence on the Internet) must understand how to protect our IP from cyberattacks. It is also important to understand the various forms of IP – as more and more organizations get into electronic commerce (E-Commerce), significantly larger number of IPs are placed on the Internet and they would be prone to cyberattacks/cybercrimes.

10.2 Intellectual Property in the Cyberspace

Intellectual Property is a number of distinct types of creations of the mind, such as inventions; literary and artistic works; and symbols, names, images and designs used in commerce.

In the legal world, IP is a generic term for legal entitlements attached to certain names, written and recorded media and inventions. Those who hold these legal entitlements may apply various exclusive rights in relation to the subject matter of the IP. The word "intellectual" indicates the fact that this term concerns a "process of the mind." The word "property" in its noun form implies that idea generation is analogous to the construction of tangible objects. Consequently, this term is controversial. Laws and enforcement about IP differ considerably depending on the jurisdiction. Inter-governmental efforts are in progress to harmonize them through international treaties – such as the 1994 World Trade Organization (WTO) Agreement on Trade-related Aspects of Intellectual Property Rights (TRIPS), while other treaties may facilitate registration in more than one jurisdiction at a time. There have been disagreements over medical and software patents. The rigorousness of copyright enforcement has so far prevented consensus on a cohesive international system. The important point is that IP laws confer a bundle of exclusive rights in relation to the particular form or manner in which ideas or information are expressed or manifested, and not in relation to the ideas or concepts themselves.

> The term "intellectual property" denotes the specific legal rights assigned to authors, inventors and other IP holders who may exercise those rights; however, the term does not denote the intellectual work itself.

Information is fluid in nature and, in the modern world, it resides on diverse networks. This has caused some confusion about how intellectual copyrights apply to files in electronic form. Long back, when world of the network users was relatively small, an emphasis on free exchange of information and a common understanding of IP created most potential conflicts over the use of information. Today networks have grown very large. There are far too many users and networks now attract a much broader range of people as compared in the past when only university and government networks were active. In such a scenario, clarification about use of electronic files becomes essential. Electronic files can be copied and distributed easily. The nature of some electronic information can create problems within existing copyright law: either the law does not address the peculiarities of electronic information or the law is too easily subverted by the ease with which files can be copied and transferred. Similar problems have arisen with photocopy machines, videocassette recorders (VCRs) and tape recorders. Matters become more complex when other countries may have other kinds of copyright laws which means that information made available globally through a network may not have the same protections in other places. IP laws are meant to protect varied forms of subject matter as mentioned below; however, in some cases there can be a degree of overlap:

1. Copyright.
2. Patent.
3. Trademark.
4. Trade Secret.
5. Trade Name.
6. Domain Name (recall the term "cybersquatting" explained in Box 1.1 of Chapter 1. It is an offense).

Let us take a look at each of these IP instances:

10.2.1 Copyright

"Copyright" is a legal concept meant to give exclusive rights to the creator of original work; usually such rights do not last perpetually – they exist only for a limited period of time. In its most general form, "copyright" is literally "the right to copy." However, it also bestows upon the copyright holder the right to be credited

Box 10.1 The Philosophy Behind Copyrights

Perhaps, the most profound and widely debated philosophical issue among scholars of copyright law is its purpose. There are different approaches – one can take the approach of looking for coherent justifications of established copyright systems. The other approach is to start with general ethical theories, such as utilitarianism (utilitarianism is the ethical doctrine that the moral worth of an action is solely determined by its contribution to overall utility) and try to analyze policy through that lens. Some people may not appreciate meaningfulness of any ethical justification for existing copyright law, viewing it simply as a result (and perhaps an undesirable result) of political processes.

There is another debatable issue – the relationship between copyrights and other forms of IP and material property. Many scholars of copyright concur that it can be called a kind of property, because it involves the exclusion of others from something. However, there is a disagreement about the extent to which that fact should allow the transportation of other beliefs and intuitions about material possessions. There are philosophical questions that come up in the jurisprudence of copyright. Such questions and issues include problems of determining situations where one work is "derived" from another, or deciding when information has been placed in a "tangible" or "material" form.

Today, we live in the era of "information revolution" and ours is an "information society" – an information society is a society in which the creation, distribution, diffusion, use and manipulation of information is a significant economic, political and cultural activity. Earlier we mentioned about "fluidity" of information that is in electronic form. We live in knowledge economy wherein a considerable opportunity exists to create wealth through the economic exploitation of information that is perceived crucial to business. The central position of IT in almost all businesses makes possible the production of such information. Information society came in existence after its predecessor – the industrial society. Closely related concepts are the post-industrial society, post-modern society, knowledge society, telematic society, Information Revolution and network society.

Therefore, any work with a copyright should not be distributed or reproduced on networks without the explicit permission of its creator (the author in most cases). Application of copyright law with this understanding is fairly straightforward. However there are other questions too; for example, with who does the responsibility for enforcing copyright protection on the networks lie?

The issue of copyright has always received much criticism and opposition. There are two broad categories in which critics of copyright fall: (a) those who assert that the very concept of copyright has never been of net benefit to society, and that it has always served simply to enrich a few at the expense of creativity; and (b) those who assert that the existing copyright regime must be reformed to maintain its relevance in the new information society.

for the work, to determine who (if anyone) can perform it or adapt it to other forms, to benefit financially from the work, and other related rights. Copyright is one form of IP (distinct from patents, Trademarks and Trade Secrets). Copyright applies to any particular expression of an idea or information which is substantial and self-contained in a fixed form. Note that the symbol for copyright is "©" (the letter C, inside circle), although used commonly, it has never been legally recognized as a symbol for copyright.

The scope of copyright does not cover ideas or information themselves; it covers only the form or style/manner in which ideas are expressed.

One important point to note is the difference between *copy protection* and *copyright protection*. "Copy protection" is a technical countermeasure while "copyright" is a legal right. Copy protection attempts to find the means for limiting the access to copyrighted material and/or inhibits the copy process itself. Examples of copy protection include encrypted digital television (TV) broadcast, access controls to copyrighted software through the use of license servers and technical copy protection mechanisms on the media. A recent example

Box 10.2 Copy Protection with DRM – Digital Rights Management

Digital Rights Management (DRM) refers to a set of access control technologies used by publishers and copyright holders in order to limit usage of digital media or devices. The term DRM may also refer to limitations associated with particular instances of digital works or devices. In a way, DRM overlaps with copy protection. The term DRM is usually applicable to creative media (music, films, etc.) whereas copy protection usually refers to software. DRM technologies are aimed at controlling use of digital media by preventing access, restricting the act of copying or conversion by end-users to other formats. Before the onset of digital or even electronic media, copyright holders, content producers or other financially or artistically involved parties had business as well as legal concerns about copying technologies. The use of DRM, nonetheless, has been contentious, that is, it is not free from controversy. One argument is that it is essential for copyright holders to stop illegal copies of their work to make sure sustainment of revenue from the work of copyright holders. On the other hand, some like to put forth an argument that "rights" is a misleading world and they suggest that an alternative term "digital restrictions management" be used. This argument is based on the position that copyright holders are attempting to restrict use of copyrighted material in ways not included in the statutory, common law or constitutional grant of special commercial use to them.

is the copy protection mechanism on digital video discs (DVDs). In open systems, however, copy protection is very difficult to achieve. On the other hand, copyright protection inserts copyright information into the digital object without the loss of quality. Whenever the copyright of a digital object is in question, this information is extracted to identify the rightful owner. It is also possible to encode the ID of the original buyer along with the ID of the copyright holder, which allows tracing of any unauthorized copies. See Appendix N in CD.

Remember that "Copyright" is an exclusive grant from the government that allows the owner to reproduce a work, in whole or in part, and to distribute, perform or display it to the public in any form or manner, including the Internet. Use of digital watermarking is one of the most well-known methods used for embedding information in multimedia data. Digital watermarks are unique identifiers embedded in digital content that makes it possible to identify pirated works. For more information, see Appendix N.

10.2.2 Patent

In simple words, a "Patent" is a document that grants the holder exclusive rights on an invention for a fixed number of years.

A "Patent" is, thus, a set of exclusive rights granted by a state to an inventor or his/her assignee for a fixed period of time in exchange for a disclosure or an invention. Through law or contractual obligation, exclusive rights can be established, but the scope of enforceability will depend on the extent to which others are bound by the instrument establishing the exclusive right. Thus, in the case of contractual rights, only persons that are parties to a contract will be affected by the exclusivity. Depending on the country of legislation, the procedure for granting patents, the requirements placed on the patentee and the extent of the exclusive rights may vary widely. The legal proceedings would be according to prevailing laws in those countries and international agreements. A typical patent application must, however, include one or more claims to support and define the invention. Such claim must be about new, inventive and useful approach or a method that has some industrial application.

The exclusive right granted to a patent holder in most countries is the right to prevent or exclude others from making, using, selling, offering to sell or importing the invention.

"Patent" is the term that usually refers to a privilege, that is, a right granted to one who invents or discovers a new method or a useful process, machine, article of manufacture or composition of matter or any new and useful improvement thereof.

"Utility patents" is the additional qualification used in some countries – for example, the US. This additional qualification is meant to distinguish them from other types of patents, but should not be confused with utility models granted by other countries. Software patents, chemical process patents, biological patents, business method patents, etc. are examples of particular species of patents for inventions. Business methods patents and software patents are relevant in the context of discussion here. Interestingly, the domain of "software patent" is most infested with trouble because software patent does not have a universally accepted definition. One definition suggested is that a software patent is a "patent on any performance of a computer realized by means of a computer program." There is an intense debate over the extent to which software patents should be granted, if at all. In the recent times, a principally active focus of the debate is the proposed EU directive on the patentability of computer-implemented inventions. This directive, known as the CII Directive or the Software Patent Directive, was ultimately rejected by the EU Parliament in July 2005. Software patents involve the following important issues:

1. Whether software is "patentable."
2. Whether software can be considered as "piece of invention."
3. Whether software patents encourage or discourage "innovation."

Probably, the issue is simpler when it comes to business method patents. These are a class of patents that disclose and claim new methods of doing business. This includes new types of E-Commerce, insurance, banking, tax compliance, etc. There is a sustained debate as to what extent such patents should be granted, particularly for inventions that are essentially legal or contractual in nature as opposed to technological in nature. Nonetheless, they have become important assets for both independent inventors and major corporations. Examples of business processes or business methods are: corporate governance, strategic management, purchasing, manufacturing, marketing and sales, etc. Next, let us understand the term "Trademark" which is yet another kind of IP.

10.2.3 Trademarks

"Trademarks" are the symbols used by businesses to identify their goods and services; government registration of the Trademark confers exclusive legal right to its use. It gives exclusive rights to use Trademark on goods and services registered to that sign and to take legal action to prevent anyone from using Trademark without consent. Thus, a Trademark is a distinctive sign or indicator of some kind that is used by an individual, business organization or other legal entity to uniquely identify the source of its products and/or services to consumers, and to distinguish its products or services from those of other entities. A Trademark is a type of IP, and typically comprises a name, word, phrase, logo, symbol, design, image or a combination of these elements.

There are also several non-conventional Trademarks comprising "marks" that are not part of standard categories. The owner of a registered Trademark may put in motion legal proceedings for challenging Trademark infringement or to prevent unauthorized use of that Trademark. However, registration is not required. The owner of a common law Trademark may also file suit – however, an unregistered mark may enjoy protection only within the geographic area where it has been used or in geographic areas into which it may be reasonably expected to expand.

The term "Trademark" is also used informally to refer to any unique attribute using which it is possible to easily identify an individual – for example, the well-known characteristics of famous actors or actresses. "Service marks" is the term used particularly in the US, when a Trademark is used in context of services rather than products.

"Ownership of the patent" is also a point to note – in most countries, patent application can be made by both natural persons and corporate entities. One or more entities then become the owners of the patent. Almost always it becomes mandatory that the inventor or inventors be named and an indication be given on the public record as to how the owner or owners acquired their rights to the invention from the inventor or inventors.

10.2.4 Trade Secret

A "Trade Secret" is a formula, practice, process, design, instrument, pattern or compilation of information used by a business to obtain an advantage over competitors or customers. In some jurisdictions, such secrets are referred to as "confidential information"; recall the discussion in Chapter 9 (Section 9.11) about information classification. An organization can protect its confidential information through non-compete non-disclosure contracts with its employees (within the constraints of employment law, including only restraint that is reasonable in geographic and time scope). The law for protection of confidential information effectively allows a perpetual monopoly in secret information – it does not expire as a patent would. The lack of formal protection, however, means that a third party is not prevented from independently duplicating and using the secret information once it is discovered. When sanction is provided for such type of information to protect it from public disclosure, it is viewed as an important legal aspect whereby a society protects its overall economic strength.

An organization invests time and energy into generating information regarding refinements of process and operation. If competitors were to get access to the same knowledge, the first company's ability to survive or maintain its market dominance would be impacted. Where Trade Secrets are recognized, the creation of knowledge is regarded as a "Trade Secret." It is entitled to be regarded as "special knowledge," that is IP. An important point to note is this – the precise language used to define Trade Secret may vary by jurisdiction as do the particular types of information that are subject to Trade Secret Protection. Although interpretations may be different, there are three factors common to all such definitions – a Trade Secret is a type of information that:

1. is not generally known to the relevant portion of the public;
2. provides some sort of economic benefit to its holder;
3. is the subject of reasonable efforts to maintain its secrecy.

Trade Secrets are not protected by law in the same manner as Trademarks or patents. Probably, one of the most significant differences is that a Trade Secret is protected without disclosure of the secret.

10.2.5 Trade Name

A "Trade Name," also known as a "trading name" or a "business name," is the name that a business trades under for commercial purposes. Its registered legal name is used for contracts and other formal situations. A "Trade Name" is also known as an "assumed name" or "corporate name." For an example, consider this: pharmaceuticals have Trade Names (e.g., Aspirin) often dissimilar to their chemical names (acetylsalicylic acid). There is a difference between "Trade Name" and "Trademark" but there are also situations where they both may be the same. As mentioned before, "Trade Name" is the name under which an organization carries out its business. A "Trade Name" identifies the business itself whereas a "Trademark" identifies goods or services or products. In some circumstances thought, it may be possible that a "Trade Name" can also serve as a "Trademark" if it meets the necessities of a "Trademark." For example "Parle" is an organization as well as a brand name. In such circumstances, the Trade Name also qualifies for the protection required under the prevailing laws. There are no exclusive rights associated with a Trade Name unless it is used as a Trademark. This stands even if the name is registered with the appropriate entity regulating business names.

A registered Trademark gives the owner the legal right to use, license or sell Trademark for the goods and services for which it is registered. A service mark is the same as a Trademark, except that it identifies and distinguishes the source of a service rather than a product. A Trademark can last as long as the owner wants, so long as the owner continues to renew the mark.

10.2.6 Domain Name

Every computer on the Internet has a unique identification number, called an Internet Protocol address.[1] Computers use IP address to find an Internet site. Internet Protocol addresses are 32-bit numeric address. As such, they are too long and not at all easy for people to remember. In order for human memories to more easily recall Internet Protocol addresses, they are "mapped," by the Domain Name System (DNS), to domain names that contain words. The registration of a domain name does not in itself confer proprietary rights to the use of that name. Associated with domain names is a phenomenon called "cybersquatting." In the US, there are Federal laws known as the Anti-Cybersquatting Consumer Protection Act. According to this law, cybersquatting means registering, trafficking in or using a domain name with bad faith intent to profit from the goodwill of a Trademark belonging to someone else. The cybersquatter then makes a higher price offer to sell the domain to the individual or organization who owns a Trademark contained within the name (see Box 10.3).

Refer to Ref. #2, Books, Further Reading to know more about IP and its various forms.

Box 10.3 Cybersquatting and Trademarks

Suppose you own a Trademark and find that someone is holding it hostage as a domain name until you pay a large sum for it, you may be the victim of cybersquatting. You can sue to get your domain name – and possibly some money damages. Cybersquatting involves registering, selling or using a domain name with the intent of profiting from the goodwill of someone else's Trademark. It generally refers to the practice of buying up domain names that use the names of existing businesses with the intent to sell the names for a profit to those businesses. In simple words, cybersquatting is the act of registering a popular Internet address, usually a company name, with the intent of selling it to its rightful owner.

The term cybersquatting is derived from "squatting," which is the act of occupying an abandoned or unoccupied space or building that the squatter does not own, rent or otherwise have permission to use. Cybersquatting is one of the most commonly used terms related to domain name intellectual property law and is often incorrectly used to refer to the sale or purchase of generic domain names. With the term "cybersquatting," however, there is a slight difference in the sense that domain names are squatted – they are sometimes paid for through the registration process by the cybersquatters.

Cybersquatters usually ask for prices far greater than that at which they purchased it. The practice that has come to be known as cybersquatting originated at a time when most businesses were not savvy about the commercial opportunities on the Internet. Some entrepreneurial souls registered the names of well-known companies as domain names, with the intent of selling the names back to the companies when they finally woke up. Panasonic, Fry's Electronics, Hertz and Avon were among the "victims" of cybersquatters. Under a 1999 Federal law known as the Anti-Cybersquatting Consumer Protection Act, you can initiate arbitration proceedings under the authority of the Internet Corporation of Assigned Names and Numbers (ICANN) and win the name back without the expense and aggravation of a lawsuit. Opportunities for cybersquatters are rapidly diminishing, because most businesses now know that nailing down domain names is a high priority.

Refer to Ref. #5, Video Clips, Further Reading, there are two links to see short video clip about protecting yourself from cybersqautting. Also refer to Box 1.1 (Chapter 1) to know more about cybersquatting.

Source: http://www.nolo.com/article.cfm/objectID/60EC3491-B4B5-4A98-BB6E6632A2FA0CB2/111/228/195/ART/ (27 January 2008).

10.3 The Ethical Dimension of Cybercrimes

When used as adjectives, the two words "ethical" and "moral" have a slight difference in their meaning. Although both words have the same origins as their noun counterparts, there is a shade of difference in meaning when used in the adjective forms.

"Moral" as a rule denotes privately good conduct whereas the word "ethical" is used to indicate a professional conduct. Moral reasons require us to respect other people as well as ourselves, to care for their good as well as our own. Moral reasons involve respecting persons through fair and just behavior with them. It also involves respecting people's rights, keeping promises, avoiding unnecessary offense and pain to people, and avoiding cheating and dishonest behavior. Morality also is expressed by caring for others and by offering help to distressed people, by expressing gratitude for favors, and by empathizing with people's suffering. Figure 10.2 puts "ethics" in context.

There are many situations of "conflicts" due to inter-relations involved (see Fig. 10.2). An individual making an ethical decision may face complexity of situation – in the capacity as a member of different groups. A software engineer or a security engineer, for example, in order to make ethical decision, interacts in many directions and within many different contexts, each of which can reflect the actual situation in a different light. For example, solving the problem on the relation among individual, colleagues and management would lead to certain choices, which may not necessarily coincide with the views of individual's family or friends, or the clients, management and other authorities, societies or other industries. Thus, ethical problems can arise when there are differences of judgment or expectations about what constitutes the true state of affairs or a proper course of action. The engineer may be faced with contrary opinions from within the firm, from the client, from other firms within the industry or from government. Figure 10.2 illustrates the complexity of situation.

Often students as well as professionals ask: What is the point in studying professional ethics? This chapter is the most appropriate place to make a comment about that. Professional ethics is not about imbibing virtue

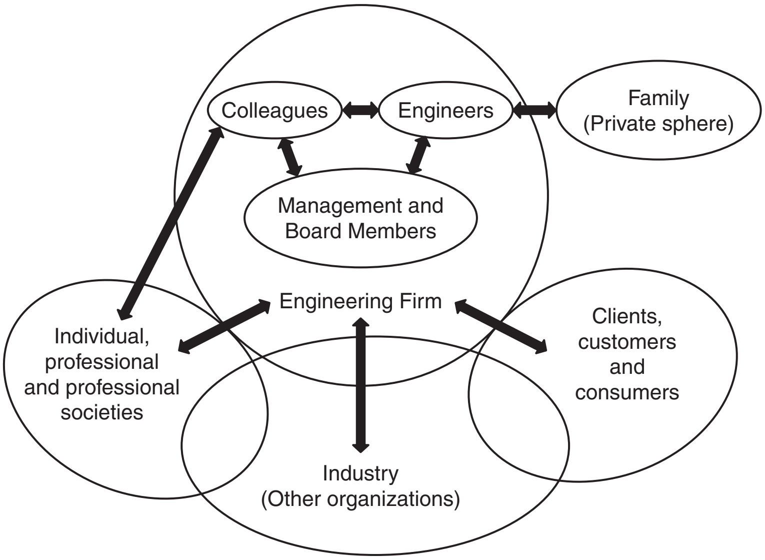

Figure 10.2 Contexts for professional ethics.

Box 10.4 Ethics and Morality

When we talk about "ethics" we refer to particular set of attitudes, values, beliefs and habits displayed by a person or a group. This sense of word is linked directly to the original sense of the Greek word ethos, which meant "customs," like "mores" the Latin root of "morals." Thus, the term "Ethics" is derived from Ethos (Greek) and "Morality" is derived from Mores (Latin). Both terms translate roughly into notions affecting "custom," "habit" and "behavior." Ethics is defined as the study of morality, which raises two questions: (a) what is morality? and (b) what is the study of morality? Morality can be defined as: *a system of rules for guiding human conduct, and principles for evaluating those rules*. However, there is a difference in the usage of adjectives "ethical" and "moral." Although the two words have the same origins as their noun counterparts, there are nuances in connotations that are probably more easily found in the adjectival forms. While "moral" as a rule refers to *privately virtuous conduct*, "ethical" is used when referring to *professional conduct*. Ethical misdeeds are actions that lead to prosecution in civil court, while moral misdeeds usually call to criminal court.

Two points are worth noting in this definition: (a) morality is a *system* and (b) it is a system comprising moral *rules* and *principles*. Moral rules can be understood as "rules of conduct,' which are very similar to "policies." Often people tend to think that "morality" is essentially private by nature and that morality must therefore be simply a personal matter. "Values" play a role in "morality." The origin of the term *value* is in the Latin word *valere*, which means "having worth" or "being of worth." Values can be viewed as objects of our desires or interests. Very general notions such freedom, love, happiness, etc. are examples of values. Societal value system gives rise to several principles. Depending on the circumstances, *ethics* and *morality* convey different and complex meanings.

There is an interesting quote on *ethics* by Abraham Lincoln:

> *There are few things wholly evil or wholly good. Almost everything ... is an inseparable compound of the two, so that our best judgment of the preponderance between them is continually demanded.*

so that the immoral and amoral individuals will adopt a certain established set of beliefs. Rather, it means to enhance the ability of concerned engineers, managers and citizens to first recognize and then responsibly confront moral issues raised by technological activity.

✍

The goal of professional ethics is to foster moral autonomy, that is the skill and habit of thinking rationally about ethical issues, as well as to improve the ability to think critically about moral matters.

The relation between "ethics" and "morality" is described is Box 10.4. Irrespective of the areas in which they are applied, the basic principles of ethics remain the same. The principles of medical ethics, legal ethics and computer ethics are similar. Theft is theft no matter whether it is an act of street robbery or done by using a computer as the instrument. New circumstances related to the computer, however, do raise new questions about how these principles should be applied. Speed, storage, identity, internationality, copying openness and availability, power mediation and privacy are the specific features of the computer that give rise to new ethical problems.

10.3.1 Ethical Hackers: Good Guys in Bad Land

The discussion in the previous section is of immense importance for the ethical hacker community. Actually, the combination of the two words "ethical" and "hacker" itself is weird because one may wonder what is "ethical" about "hacking." However, it is a common practice now for organizations to invite professional hackers and pay them fees for testing the security of their IT infrastructure, especially for the Web-based applications and portals. "Ethical disclosure" is a terminology used in the ethical hacking domain. The ethical question is this: suppose an ethical hacker finds certain vulnerabilities in the software developed or website designed for an organization that has hired the ethical hacker. After waiting for a requisite time, the hacker does not get any response from the organization indicating their action plan and date for closing the gap found (i.e., vulnerability), then in the interest of getting the gap closed, should the ethical hacker throw open the known vulnerability to the public hoping that some third party may offer a solution to close the vulnerability? This is indeed an ethical issue because by making it known to the "public," as much as the "good guys" acting on it, the hacker community also becomes aware of the weakness/vulnerability and they may as well make plans to exploit that vulnerability. This is indeed a point to ponder for ethical hackers – moral responsibilities of ethical hackers.

Ethical hackers are required for many reasons and they are hired by organizations.

In Chapter 12 (in CD), guidance is provided about certification exams in this domain, that is, the CEH (certified ethical hacker). With the growth of the Internet, computer security has become a major concern for businesses and governments. Both governments and businesses want to make good use of the Internet for E-Commerce, advertising, information distribution, access and other pursuits. However, they are worried about the possibility of being hacked. Along the same lines, the potential customers of these services are concerned about maintaining control of sensitive information – for example, credit card numbers, social security numbers (SSNs) and home addresses; add to this the privacy concerns. Organizations realize that one of the best ways to evaluate the intruder threat to their interests would be to have independent computer security professionals attempt to break into their computer systems. This idea is similar to having independent auditors engaging with an organization for verification of practices as per adopted standards. In the context of computer security, these "tiger teams" or "ethical hackers" would use the same tools and techniques as the intruders, but they would neither damage the target systems nor steal information. Instead, they would evaluate the security of target system and would report back to the owners with the vulnerabilities they found.

According to a popular myth, hackers are mischievous adolescents or desperado groups who ply their alchemy in the shadows of cyberspace. Hackers are often shunned for being the instigators of criminal computing offenses; however, very few may know that hacking actually began as a way of playing with technology and finding better ways to use it. There was a time, when only a select few knew the secrets of software. A revolutionary time came after the PC was unleashed by IBM. After that computer became accessible to people and by now an average 14-year-old may be more adept at cracking codes than the middle age CEO of multi-billion dollar company. So, let us attempt to understand the mind of hackers. Economic impacts of cybercrimes have been dwelt well upon in the previous chapters. The costs associated with cybercrimes are described in Chapter 9 (Section 9.2) in terms of the impact they have on organizations.

Information technology has made tremendous progress in the past four decades and IT has become an integral part of our life – personal life as well as professional life. We cannot imagine life without computers; especially in the metropolitan area. Mobile hand-held and wireless connectivity devices have become haunting objects in modern life; they are omnipresent! Even then, in most cases today, we are still able to decide for ourselves whether we want to use devices equipped with modern computer technology (e.g., by manually controlling our central heating system, or by choosing not to carry a mobile phone if we dislike the constant accessibility its usage implies). As we embrace computers, we keep more and more data on it and some of that data can be confidential. Computers no more stand in isolation; they are heavily networked in the Internet era. We learned in the previous chapters how cybercriminals take advantage of this fact. Motives of hackers are depicted in Fig. 10.3 – it is a good starting point for the rest of the discussion in the chapter.

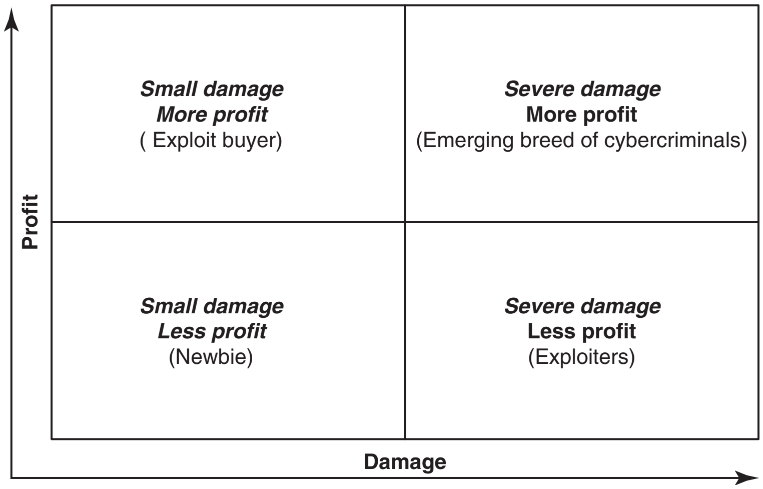

Figure 10.3 | Hackers' motives (profit and damage).

Box 10.5 Computer Ethics

Ethics is one aspect of practical philosophy to explain how professionals in computing domain should make decisions about professional and social behavior. Ethics is a set of moral principles that govern the behavior of a group or individual. Computer ethics is set of moral principles that control the use of computers. Some common issues of computer ethics include intellectual property rights (such as copyrighted electronic content), privacy concerns and how computers affect society. The term "computer ethics" was first coined by Walter Maner in the mid-1970s. Since the 1990s the term started getting integrated into professional development programs in academic settings. The conceptual foundations of computer ethics are investigated by information ethics, a branch of philosophical ethics established by Luciano Floridi. For computer applications domain, "computer ethics" is an important topic. Since the 1990s the importance of computer ethics has increased. With the growth of the Internet, privacy issues as well as concerns regarding computing technologies such as Spyware and web browser cookies have raised the question about ethical behavior in technology. In the computer technology domain along with the related domain of information security, the mention of ethics is important given that computers are special technology and they raise some special ethical issues. A typical problem in computer ethics arises because there is a policy vacuum about how computer technology should be used.

The name "computer ethics" was not commonly used until the mid-1970s when Walter Maner began to use it. He defined this field of study as one that examines "ethical problems aggravated, transformed or created by computer technology." In the book, *Computer Ethics* published in 1985 it was said that computer ethics is a branch of studies focusing on the way in which computers "pose new versions of standard moral problems and moral dilemmas, exacerbating the old problems, and forcing us to apply ordinary moral norms in uncharted realms." Computer ethics has two parts: (a) the analysis of the nature and social impact of computer technology and (b) the corresponding formulation and justification of policies for the ethical use of such technology.

The 10 commandments of computer ethics created by the Computer Ethics Institute match well within the context of computer legislations across the world.

[1] Thou Shalt Not use a computer to harm other people;
[2] Thou Shalt Not interfere wth other people's computer work;
[3] Thou Shalt Not snoop around in other people's computer files;
[4] Thou Shalt Not use a computer to steal;
[5] Thou Shalt Not use a computer to bear false witness;

Box 10.5 Computer . . . (*Continued*)

[6] Thou Shalt Not copy or use proprietary software for which you have not paid;
[7] Thou Shalt Not use other people's computer resources without authorization or proper compensation;
[8] Thou Shalt Not appropriate other people's intellectual output;
[9] Thou Shalt think about the social consequences of the program you are writing or the system you are designing;
[10] Thou Shalt always use a computer in ways that insure consideration and respect for your fellow humans.

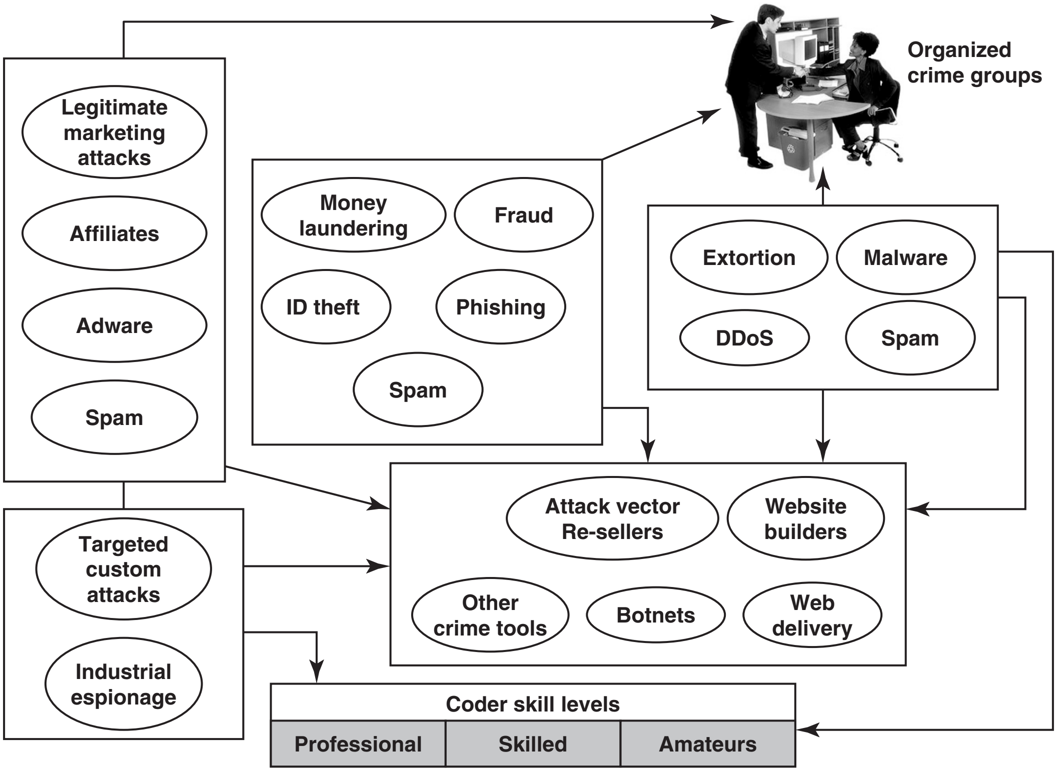

Figure 10.4 Cybercrimes – the connections and syndicates.

As we can see in Fig. 10.3, cybercriminals are getting bolder; they are going for bigger gains these days; they will not think twice even if their attacks result in severe damage to the impacted party. They are willing to take the associated risks. This perhaps could be due to the fact that even hacking is becoming an organized business and there are many syndicates involved – see Fig. 10.4.

Information in cyberspace can be accessed globally and in such a milieu"computer ethics," helps us examine what is right and wrong for the Internet users, and social impacts of information technology (IT) in general. As mentioned before, "Intellectual Property" (IP) means creations of the mind, such as inventions; literary and artistic works; and symbols, names, images and designs used in commerce. Software piracy is an IP violation crime.

10.4 The Psychology, Mindset and Skills of Hackers and Other Cybercriminals

Information is a source of power and many perceive that holding "information" or for that matter "confidential information" is the key to prosperity that comes with access to that information. For example, protected health information (PHI), which is worldwide considered as sensitive personal information (SPI), is stolen because those who steal it see an appeal in it – there are people in the market who would like to buy it. For instance, list of major patients of a large hospital would hold much appeal to the competitors. List of key account holders of a bank would, similarly, hold value in the eyes of the bank that is a competition and so on. Similarly, "voters list" in an area could be seen as valuable for an electoral candidate who may want to use it for his/her campaigning; of course, in this case, it could be a public domain information and, therefore, the efforts involved in obtaining it could be much less. For CRM applications, the list of customers of a major retail business would be much sought for. Thus, we can see the motives involved in stealing the information. Those who steal it know that they have stolen it and that there are laws and legal frameworks (as seen in Chapter 6) and yet the criminals are not worried about the law catching them! Perhaps they think that they can get away with it? Interestingly, cybercriminals tend to operate as a close-knit community – therefore, it is felt that cybercrime is now becoming an organized crime! (see Fig. 10.4).

E-Goverance is getting well established as electronic systems have now reached into all levels of government, into the workplace and into private lives to such an extent that even people without access to these systems are affected in significant ways by them. New ethical and legal decisions are necessary to balance the needs and rights of everyone. With advanced computer technology, it is important to understand computer ethics related to security, privacy issues and major negative impacts of IT. Read on the next section and think if there is a shade of "goodness" in terms of any difference between the hacker community (see Fig. 10.5) and downright cybercriminals. We take you through "generations" of hackers and the characteristics of each generation.

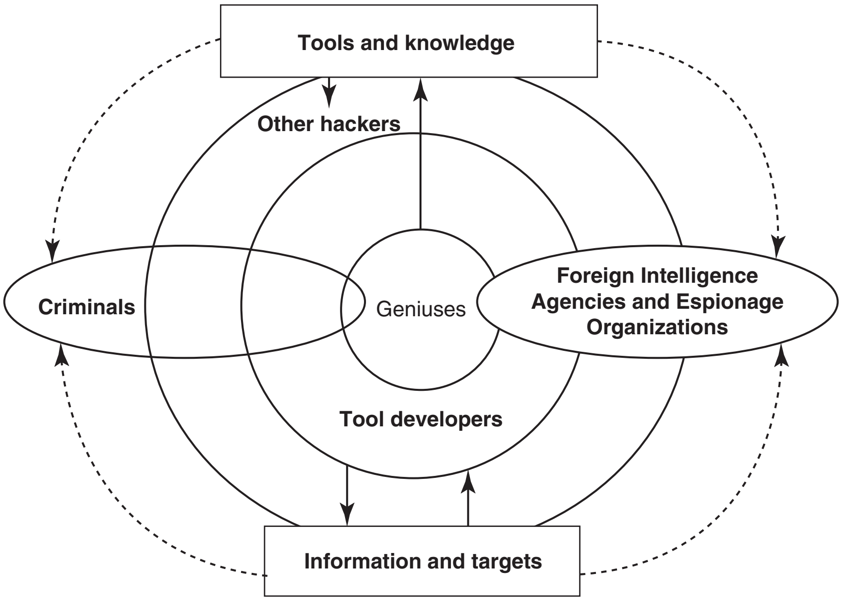

Figure 10.5 Hackers community.

10.4.1 Inside the Minds and Shoes of Hackers and Cybercriminals

Some hackers view their activities as being "value-free," without distinguishing between good hacking (like the ethical hackers are paid to carry out hacking for an official purpose) and bad hacking (meant for causing trouble to others though hackers feel it is for satiating their technical and intellectual appetite).

> One popular view among hackers, which may sound eerie to us is, "breaking into a computer should not be a crime because no one gets hurt and we all learn something." A more daring motto of hacker motto be "Don't get caught," along with the caveat, "and if you do get caught, cash in and make money."

The basic motives behind web attacks and hacking are: (a) money, (b) freedom, (c) love, (d) personal gain:

1. **Money as the motive:** Majority of hackers get into cybercrime for monetary gain. Money is the primary motivation behind cybercrime whether it is stealing people's bank account information, fraudulently obtaining money or property by altering computerized information. In one of the biggest frauds that history has seen, Gonzalez was the mastermind behind the combined credit card theft and subsequent re-selling of more than 170 million credit cards and ATM numbers from 2005 through 2007. See illustration 5, Chapter 11 in CD. In addition to the card numbers bogus passports, drivers' licenses, SSNs, birth certificates, college student identification cards, health insurance cards were also sold at auction!
2. **Freedom as the motive:** Many hackers believe that the Internet should be free and that all computers should be completely accessible. They could also have a political or social agenda where their aim is to damage high-profile computers to make a gain. These types of hackers are also known as *hacktivists*, or *Neo Hackers*. In general, most hacktivism involves defacement of website or denial-of-service (DoS) attacks. In extreme cases, hacktivism is used as a tool for cyberterrorism.

   The British hacker Gary Mckinnon went unnoticed for years while he was hacking NASA, the US Army, US Navy, Department of Defense and the US Air Force. Mckinnon at that time was considered the biggest military computer hacker of all time. His claim is that he was being studious. His argument was that he was looking for evidence of UFOs, antigravity technology and the suppression of "free energy." US authorities, however, claimed that Mckinnon deleted critical files from operating systems. This, they said, resulted in the shut down the US Army's Military District of Washington's network of 2,000 computers for 24 hours, as well as deletion of US Navy Weapons logs, rendering a naval base's network of 300 computers inoperable after the September 11 terrorist attacks. US authorities claim these travails of Mckinnon cost them $800,000 to track and correct the problems he caused. McKinnon, however, has denied causing any damage, arguing that, in his quest for UFO-related material, he accessed open unsecured machines with no passwords and no firewalls and that he left countless notes pointing out their many security failings. He obstinately disputes the damage and the financial loss claimed by the US as concocted in order to create a dollar amount justifying an extraditable offense.
3. **Love as the motive:** This sounds wonderful and it is also one of the motives. Being in love has prospered many and being in love has destroyed many! Life is smooth until you become suspicious of your boyfriend's/girlfriend's fidelity. On the Web, many spying and hacking resources are available for those trying to "catch a cheater."[2] Those with a poisoned mind about their partner, suspecting that a boyfriend or girlfriend, wife or husband might be double playing with them, use computer hacking knowledge. They do this as a punishment! The one, who has the feeling of being cheated, goes all out to tap into his "suspected" partner's computer!

There is well-known case where the scenario goes something like this – a lady's divorce case is filed and is in progress. She collects information on affordability for husband to pay the maintenance charges. She gathers (to support as evidence) information of financial nature by hacking into his bank account! She also finds a lot of similar evidence of digital nature. It turns out later that husband had shared the password for online bank account! The lady also collected evidences from her father-in-law's account; however, the father-in-law had not shared his password. An interesting question is whether as per the Indian Evidence Act, it matters HOW the Evidence is gathered (refer to Appendix Q – The Indian Evidence Act in CD). Hacking is illegal by IT Act – so while the lady may be granted the divorce, she could end up in jail. This example is mentioned here only to illustrate the point about "being cheated" in love or relationship, acting as a motive to hack.

4. **Personal gain as the motive:** In hacker community, a "*script kiddie*" or "*skiddie*" is often assumed to be a juvenile using script developed by others to attack computer systems and networks either to impress friends or gain credit in computer-enthusiast communities. An 18-year-old high school student from Minnesota, Jeffrey Lee Parson, was responsible for spreading a variant of the infamous Blaster computer worm. Using a hex editor, Parson only modified the original Blaster worm that was already prevalent. He added his screen name to the existing executable, and then attached another existing backdoor, *Lithium*, and posted it on his website. Through this subtle modification, authorities were able to trace the name back to him. The program was part of a DoS attack against computers using the Microsoft Windows operating system. The attack took the form of a SYN flood which caused only minimal damage. In 2005, Parson was sentenced to 18 months in prison.

10.4.2 Hackers and Cybercriminals: Evolution of Technical Prowess and Skills

Just like oriental sport "Karate" (the black belt, the green belt, etc.), there are several levels of expertise in hacking. These levels are known as "Black Hat Hacker" and "White Hat Hacker" – refer to Box 2.2 in Chapter 2. There are also "generations of hackers." For example, the first generation in 1960s was the creative programmer breed. The second generation in 1970s was termed as the computer evolutionary generation. The third generation in 1980s was the games and copyright breakers. The 1990s saw the rise of fourth generation – the criminals and cyberpunks (see Box 1.1 of Chapter 1 where the term "cyberpunk" is introduced).

Each generation is characterized by their own achievements (negative though!). For example, the *first generation* worked more like creative programmers and scientists. They employed novel methods for programming, known as code bumming. They did have some sense of ethics, that is,. they would do the right thing within their sphere of work. They were considered "Gurus" and were respected.

The *second generation* was considered the "computer evolutionaries." They were more of hardware hackers and they used computer kits such as Altair and Apple. Later the people from this generation became founders of many companies. It was the beginning of "phreaking" and "software piracy."

The *third generation* went into computer games and copyrights domain. They enjoyed developing methods for protecting and breaking copyright codes on games. Their work involved minor criminal activity. Personal PCs dominated their era and they were in a big way into computer-based entertainment software to hack computer games. That was the end of "Technical Guru" type of generation.

The fourth generation is truly the "criminal" generation and "cyberpunks." This generation is not said to be technically as elite as the previous generation. Hackers of this generation are criminally oriented and motivated primarily by greed, power, revenge, malicious intent (see Fig. 10.3). It is no surprise then that this generation is not respected. Figure 10.6 represents the sophistication of attacks from 1950s to date. In a 2008 survey,[3] it was estimated that 67% of those who engage in web attacks are profit-motivated.

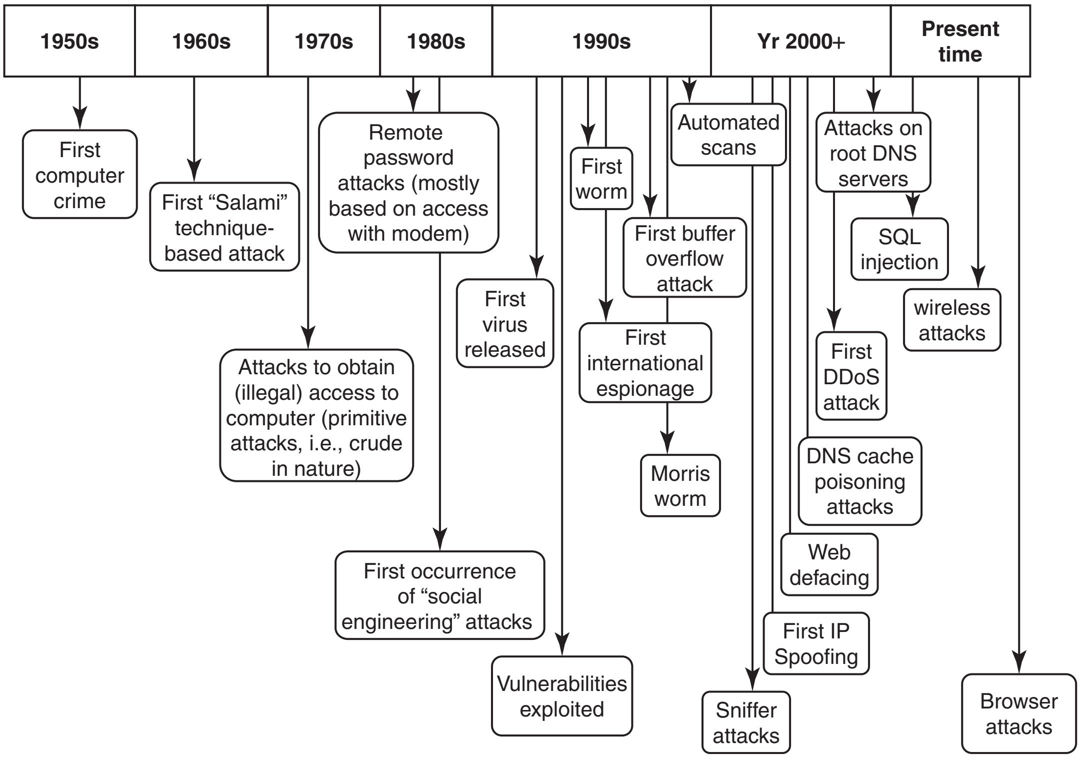
1950s
1960s
1970s
1980s
1990s
Yr 2000+
Present time
First computer crime
First "Salami" technique-based attack
Attacks to obtain (illegal) access to computer (primitive attacks, i.e., crude in nature)
Remote password attacks (mostly based on access with modem)
First occurrence of "social engineering" attacks
First virus released
Vulnerabilities exploited
First worm
First international espionage
First buffer overflow attack
Morris worm
Automated scans
Sniffer attacks
First IP Spoofing
Web defacing
DNS cache poisoning attacks
First DDoS attack
Attacks on root DNS servers
SQL injection
wireless attacks
Browser attacks

Figure 10.6 | Sophistication of hacker attacks.

When we think about the mindset of hackers, we realize that the hacker community must be quite a studious community in a technical sense; they spend quite some time in "information gathering." They "sniff" the network traffic; "listen" to the network traffic as part of "passive" phase in their further warfare plans! Recall the discussion in Chapter 2 (Sections 2.2.1–2.2.3) about "reconnaissance" (information gathering), "passive attacks" and "active attacks." This studious community called "hackers" is a technologically advanced community; some of the tools they use are mentioned in Table 2.2 of Chapter 2. Those tools are of two types: (a) Reconnaissance tools and (b) exploitation tools. *Reconnaissance* often begins with searches of Internet databases including Domain Name System (DNS) registries, Whois databases, Google, online news sources, business postings and many other online resources. The reconnaissance phase often includes print media as well, specifically electronically searchable archives that would be found at a college library or large public library. *Exploitation tools* are used to verify that an actual vulnerability exists by exploiting it. It is one thing to have vulnerability testing software or banners indicating the possibility of an exploitable service, but quite another to exploit that vulnerability. Some of the tools in this category are used by both attackers and penetration testers. Many tools in this category are single purpose tools that are designed to exploit vulnerability on a particular hardware platform running a particular version of an exploitable system. The tools mentioned in Table 2.2, Chapter 2 are unique in the sense that they have the ability to exploit multiple vulnerabilities on a variety of hardware and software platforms. "Metasploit" is a tool that attackers would use to take over, or own, a computer. There are many more tools available than those mentioned in Section 2.2 and Table 2.2 of Chapter 2.

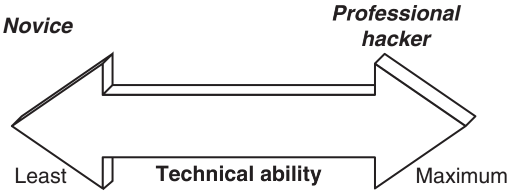

Figure 10.7 Hacker technical skills continuum.

In the introduction section, some terms were mentioned – novice, newbies\script kiddies, insiders, cyberterrorists, political activists, etc. They are alternate terms for hackers and cybercriminals. In terms of knowledge, skills, competence and abilities, there is a large range in this domain – see Fig. 10.7. The *novice* (also known as newbie/script kiddies) has limited computer skills. They are new to the circuit and they tend to heavily rely on software available on the Internet. Their work can best be described as "nuisance attacks" such as the denial-of-service (DoS) attacks described in Section 4.9 of Chapter 4. In a strange sense a "novice" can be more dangerous than the "Pros" because they can cause extensive damage to systems due to their limited technical skills (refer to Fig. 10.7) they do not understand how the attack works. They are hungry for attention, especially media attention and we know that the media these days is very aggressive and inquisitive as well as exploitative.

Media people love scare stories. For example, digital discrimination, corporate misbehavior, loss of privacy, loss of anonymity, etc. In short, they are like "big brother is watching you"! The media also drew attention to the fact that some of the terrorists involved in the 9/11 attacks were known faces, and if there had been biometric face recognition software in use at airports, the situation could have been diluted or even prevented. This schizophrenic approach to the issues only highlights why ethical considerations in computing are so important.

Cyberpunks (refer to Box 1.1 in Chapter 1) are next in the skills and competencies continuum. They have better computer skills although they typically have limited programming knowledge. However, their understanding about how cyberattacks work is better. They have criminal intent, malicious behavior and they too seek media attention. Typical frauds done by these criminals are found to be credit card frauds – in Section 11.4.2 in Chapter 11, several illustrations are provided about the kinds of frauds that cyberpunk indulge themselves in. The *insiders* are the least suspected ones because organizations and individuals trust them by the very fact that they are "insiders"! This genre of criminals is technically suave and computer literate. They dabble in technology/information field. As industry experience shows, most times, they are disgruntled current employees or ex-employees who have a strong urge for taking "revenge" because they believe that they have been wronged, that is, they believe that some injustice has been done to them. Most times, they succeed in carrying out cyberattacks due to their privileges inherent in the position they occupy in their organization. Refer to the Brainvisa case[4] – it is live demonstration of how insiders can exploit the security weakness and trust of their organizations. Access rights must be managed well with only "need-to-know" as the basis for granting or declining access. In this case, apparently the top management member had the access to source code and he then misused it.

The next category of cybercriminals comprises the *coders.* Coders are technically skilled. They write the scripts and automated tools and act as a mentor to the "newbies" mentioned earlier.

Coders are motivated by a sense of power and prestige. They are revered in their community but dangerous to us as they have hidden agendas such as writing deadly codes a Trojans, etc.

The "professional hackers" mentioned in Fig. 10.7 are criminals and thieves. They are often involved in corporate espionage. They work like mercenaries, that is, "guns for hire." They are highly motivated, highly trained and have the right ammunition (i.e., state-of-the-art equipment) but unfortunately all for the harmful purpose. They have a lack of respect for other people's information property. They work as a close-knit community and operate mostly underground. Read Xiao Chung's Story "Life of a Hacker" mentioned in Example 21 in Section 11.2.21 in Chapter 11. The ultimately dangerous category in terms of knowledge, skills and competencies in the cybercrime world is the "cyberterrorist" (refer to Box 1.1 and Section 1.2 in Chapter 1). There is an increase in cyberterrorism activity since the fall of many Eastern Block intelligence agencies.

Cyberterrorists are well funded and they are also quite very motivated (although for wrong purpose). They thrive due to the opportunities they get for mixing political rhetoric with criminal activity.

Unfortunately, very little is known in this area; to know more read Molander, Riddile and Wilson "Strategic Information Warfare" mentioned in References.[5]

10.4.3 Ethical Hackers

As mentioned before, there are categories of cybercriminals and hackers based on the continuum of their skills and competencies (Fig. 10.7). Researchers believe that there are certain traits possessed by this community, mainly due to their mental disorders.

Box 10.6 Understanding Ethical Hacking

In Chapter 2 (Box 2.2) there was a mention of "white hat hacker." A white hat hacker is an "ethical hacker," that is, the "good guy." An ethical hacker is a computer and network expert who attacks a security system on behalf of its owners, seeking vulnerabilities that a malicious hacker or intruder could exploit; so, in a way, this is like "vulnerability scanning" and "penetration testing." In order to "test" the goodness of a security system, ethical hackers use the same methods as their less principled counterparts, that is, the "bad guys" who hack for malicious intentions – the only difference is that ethical hackers report the vulnerability problems noted instead of taking advantage of them. Ethical hacking is also known as penetration testing, intrusion testing and red teaming.

Ethical hackers are technically sound professionals; they possess a variety of knowledge and skills concerning the Web, network and operating systems (OS), programming and physical security. However, in order for the organizations to entrust this "planned hacking," first and foremost, ethical hackers must be completely trustworthy. Depending on the sensitivity of the information gathered during an evaluation, strong measures need to be taken to ensure the security of the systems being employed by the ethical hackers themselves. When you choose to work with ethical hackers, it is important that you select companies that are leaders in their field and therefore in order for, you to trust that your information will be protected. These organizations understand the sensitivity of the information gathered at the client organization during an evaluation and have strong measures in place to ensure the security of the data. Basically, ethical hacker seeks to answer some basic questions:

1. To what information, locations and systems an intruder can gain access? What is being protected?
2. What are you trying to protect against?
3. When an intruder gains access, what can he/she see on the target facilities, networks and systems?
4. What can an intruder do with that information and data?
5. Does anyone at the target notice the intruder's attempts or successes?
6. How much time, effort and money are you willing to expend to obtain adequate protection?

Most hackers, by personality, are socially inept, obsessive in behavior. Most are loners and yet they seem to crave for "membership," "inclusion," "recognition," etc. They have inferiority complex and are escapists. Most hackers have some kind of "computer addictive disorder."

"Hackers" would not agree with this – they feel that as long as there is "curiosity" and the need to "explore," there will be hackers. Hackers believe they are computer security professionals and that their work involves high "intelligence"! They believe that security professionals get their salaries because there are hackers! In Refs. #2 and #3, Additional Useful Web References, Further Reading we have provided some links to read about how the minds of hackers work.

When employing "ethical hackers," certain care must be taken by organizations. The person employed as an ethical hacker must be completely trustworthy.

It is important to understand the skill-sets as well as "mindset" to look for while employing "ethical hackers." First and foremost, the person employed as an ethical hacker must be completely trustworthy. While testing the security of a client's systems, the ethical hacker may discover information about the client that should remain secret. In many cases, this information, if publicized, could lead to real intruders breaking into the systems, possibly leading to financial losses. During a security evaluation, the ethical hacker often holds the "keys to the company." Therefore, he/she must be trustworthy enough to exercise tight control over any information about a target that could be misused. The sensitivity of the information gathered during an evaluation may dictate strong measures be taken to ensure security of the systems being tested by the ethical hackers. Certain areas to watch are – limited-access laboratories with physical security protection, multiple secure Internet connections, a safe to hold paper documentation from clients, strong cryptography to protect electronic results and isolated networks for testing. Ethical hackers normally have strong programming skills

Box 10.7 The Hacktivist

There is also another interesting term known as the "hacktivist." Hacktivism is the act of hacking or breaking into a computer system for a politically or socially motivated purpose. The individual who performs an act of hacktivism is said to be a hacktivist. A hacktivist uses the same tools and techniques as a hacker, but does so in order to disrupt services and bring attention to a political or social cause. For example, one might leave a highly visible message on the home page of a website that gets a lot of traffic or that embodies a point of view that is being opposed. Some examples are shown in Figs. 1.9 and 1.10, Chapter 1. Or one might launch a denial-of-service (DoS) attack to disrupt traffic to a particular site.

As another example of hacktivism, consider the following: hacktivism following the death of a Chinese airman when his jet fighter collided with a US surveillance plane in April 2001. Chinese and American hacktivists hacked websites and used them as "blackboards" for their statements. The legal side seems intriguing because according to law professionals, whether hacktivism is a crime may be debated. Opponents argue that hacktivism causes damage in a forum where there is already ample opportunity for non-disruptive free speech. Others insist that such an act is the equivalent of a protest and is, therefore, protected as a form of free speech.

Source: To know more about hacktivism, visit the following sites:

1. http://en.wikipedia.org/wiki/Hacktivism (2 January 2008).
2. http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci552919,00.html (2 January 2008).
3. http://www.thehacktivist.com/?pagename=hacktivism (2 January 2008).

and computer networking knowledge. Typically, ethical hackers have long work experience in computer and networking business. They are also proficient in installing and maintaining tools that use the more popular operating systems on target systems. These base skills are augmented with in-depth knowledge of the hardware and software available from popular computer and networking hardware vendors. An additional specialization in security may not always be necessary, because strong skills in the other areas imply a very good understanding of how the security on various systems is maintained. These system management skills are necessary for the actual vulnerability testing, and are equally important when preparing the report for the client after the test. Globally, the hiring of ethical hackers is on the rise with most of them working with top consulting firms. See Chapter 12 (in CD) for related certification information.

10.5 Sociology of Cybercriminals

In the previous section, we described about the mind-set and skills and competencies of hackers and cybercriminals. Are these people "socially disturbed"? A study of hackers shows that hackers, young and old, have their own reasons to feel alienated in society, one of which is the misrepresentation of their faith in the media. Originally "hacking" involved only feeling passionate about writing software to the extent of pursuing this interest sometimes outside the norms, which would not necessarily imply anything illegal.

The original "hackers" such as Richard Stallman were employees of respectable institutes such as the Massachusetts Institute of Technology (MIT). As such with their association with respectable institutes, they could hardly be seen as being "outside" the system. During 1980s, however, there was a boom in computer science research. It was caused by projects sponsored by the military organizations; projects such as Strategic Missile Defense and Artificial Intelligence. With that, the mood in these research ivory towers, which had been fairly liberal in the 1970s, changed. Mavericks like Stallman left, and hackers outside the state-sanctioned system were increasingly perceived as a potential threat to national security.

From the mid-1980s onward, secret services and other law enforcement agencies started their "war against hacking," with a compliant mass media doing their best to stigmatize hackers as criminals, or even as terrorists. In the 1990s, with the mass adoption of the Internet, a new breed of hackers emerged, so-called "script kiddies" (described in the previous section). This breed of people did not have to develop deep knowledge of computers because hacking tools had become relatively easily obtainable.

Script kiddies are not considered as real hackers but instead they are called *crackers*.

Script kiddies have a mania for breaking into web servers, obtaining "root" privileges and inscribing digital graffiti on the web server's homepage. This activity served as legitimating for the strengthening of the legal regime, and allowed centrally owned mass media to continue, in full force, their denouncement of computer subcultures in general.

10.5.1 Personality Traits of Cybercriminals and Young Generation's Views about Hacking

There was an interesting research carried out in year 2006 by Purdue University.[6] It seems that there is a gender difference – as per that study, 87% of the respondents were male and only 13% were female! They were the 77 students from a Midwestern University enrolled in courses at the college of technology. The mean age of these participants was 21 years. The hypothesis for this study was that individual's self-reporting deviant computer activities (classified as computer criminals for this study) would be more introverted, more open to experience, more neurotic, more exploitive and manipulative and would score lower on social moral choice as compared to the other group under study, that is, those individuals having self-reporting non-deviant/computer criminal behavior. The result of this study showed that 88% of respondents were classified as computer criminals. The results also showed that only extraversion total was noteworthy in relation to deviant/criminal computer behavior, none of the other hypotheses were supported. The finding that low extraversion (introversion) was a major predictive variable is contrary to previous research. The finding that moral reasoning was not a significant variable is also contrary to other studies concluding that a lack of internalization of societal norms was a significant factor in unethical and aberrant computer behavior.

It looks like the young generation in India has a certain viewpoint toward hacking. There are opinion polls indicating that most young people in India and worldwide believe that hacking is a good skill and that every programmer and software designer should know how to prevent hacking. Therefore, knowledge about how hackers work is an essential knowledge in the opinion of India's young generation. Another school of thought heard from young generation is this:

> *If thieves, enemy countries, enemies, terrorist groups and other ill-fated people and organizations can use 'Hacking' for their means of destruction, why cant authorities use hacking as their tools for protection? While these ill-fated hackers constantly try to hamper the smooth living and lifestyle of common man, why cant authorities recruit hackers to stop them from doing these and even take precautionary measures? This can be accomplished by developing hacking and tracking software tools and techniques through which these BAD HACKERS can be traced before they do anything wrong.*

We should take the positive side of these issues and approach as required and help our government and institutions.

10.6 Information Warfare: Perception or An Eminent Reality?

Computer networks are becoming the battle ground for economic warfare in the modern times. The role of the computer as a weapon in and of itself magnifies the potential for Information Warfare (IW). Everyone knows that hacking is a crime.

Most countries are now using the technique of "Information Warfare" (IW) for capturing the information of enemy countries. This technique is also used by the professional high-profile techno-thieves. In some cases, the victim never knows that he has been hacked. So there is enough need for understanding the symptoms and its effects on hacking. There should also be knowledge of availability of different tools that are in the market and the tools that can prevent from being hacked.

More than guns, bombs or missiles, the Internet is the most important tactical tool for terrorist groups today. "Asymmetric warfare" involves unconventional weapons coupled with innovative strategies aimed at attacking the will of the target with full effort to cause maximum damage. Asymmetric warfare is used by terrorists, the media and hackers. The concern is that the virtual free rein terrorists currently have over the Internet, is allowing them to plan large-scale attacks against civilian targets, while policymakers continue to worry primarily about a cyberattack on the nation's information infrastructure. Limiting the ability of terrorist networks to use the Internet as an operational platform is one of the most significant challenges that

Box 10.8 Information Warfare Classification

Information warfare and information warfare incidents can be segregated into three classes:

1. Personal information warfare.
2. Corporate information warfare.
3. Global information warfare.

This classification depends on the target, that is, whether the subject of the attack is an individual, business enterprise or government, respectively. Information warfare has a close nexus to infrastructural warfare, which involves interference with a government without essentially a direct impact on day-to-day life. As more computers connect to systems used by the society as a whole, the capability to use computers to engage in infrastructural warfare will only increase.

Using computers for performing calculations in development of the hydrogen bomb, breaking of the enigma code in Bletchely Park and in Aiken, and Jon Von Neuman's automated generation of ballistic tables etc are some of the famous examples of information warfare involving use of advanced technology. Over the decades, sophistication of applications and the prowess of underlying computer technolgoy has advanced considerably. Today, computers are commonly used for command and control systems in the modern, digitized battlefield. Initially, computers were developed for calculational purpose and today, they are being considered as war weapons! Not many years back, an incident was uncovered wherein Dutch hackers got hold of sensitive information including order-of-battle data. They got to this classified information by penetrating information systems of Coalition Forces during the Persian Gulf War. This information, perceived as highly valued, was offered to the Iraqi government for a price!

lawmakers and national security experts face. It is said that all is fair in love and war – this saying seems to be followed. Corporations actively participate both as targets and possibly also as combatants.

The idea that you can attempt to disrupt and break into foreign information technology is not new. It dates back as far as the British code breakers who figured out the Nazi "Enigma" encryption machine in World War II. The adversaries have changed over the years, but their struggle has kept pace with the development of cyberspace, and it continues today. A reading of the military and non-military literature reveals that the term "information warfare" (IW) is at best a label of loose connotations. The connotations of IW range from specifically technical tactics (e.g., hacking) through more subtle manipulations (e.g., psychological operations) to a broad epochal boundary in techno-military history. One of the great ironies of the Internet era is that the very characteristics of the Internet, which appeal to government, industry and private users, are some of the same dynamics that make it an ideal operational headquarters for contemporary global terrorist movements. Like any Internet user, a terrorist operative will find setting up a website or E-Mail account to be a very simple and inexpensive process. With minimal disclosure requirements (which are difficult, if not impossible, for providers to verify for accuracy), a cyber jihadist[7] can set up any number of free E-Mail accounts within a matter of minutes.

10.6.1 Cyberwar Ground is HOT

Almost everyday, there is news about cyberattacks; intensity of cyberattacks mirrors the intensity of fighting on the ground. Core attackers are few in numbers and they lead by providing ideas, websites and tools. Volunteers and conscripts are thousands in number; they do the brute force work. They come from all over the world (see Fig. 10.6). There are examples of many government sites hacked – refer to Figs. 1.7, 1.9 and 1.10, Chapter 1. Grabbing the mouse is a lot easier than grabbing the gun! Military training requires arduous efforts; use of computer does not! There are opportunistic participants and "hacktivism" (see Box 10.7) gives everyone a chance to impact the course of history. The two prominent weapons in IW are (a) DoS attacks and

(b) website defacements; refer to Chapter 1 (see Figs. 1.7, 1.9, 1.10) – business loses revenue and governments lose face. Cybertools used by cyberattackers are – Ping of Death, EvilPing, Ping-flood (mainly for launching DoS and DDoS attacks) and Winsmurf, QuickFire, Defend, HTTP Bomber 1.001b, FakeMail, MailBomber, Attack 2.5.1, PutDown. A new attack method involves, requesting non-existent webpages, specifying current date/time. This way, a cyberterrorist defeats web-caching security mechanisms. Typical targets in information warfare involving cyberterrorists are: websites, E-Commerce servers, E-Mail servers, Internet relay chat (IRC) channels, WWW chat rooms, Domain name servers (DNS), Internet service providers (ISPs), File Transfer Protocol (FTP) sites, etc. Chapter 4 has the details of tools and methods used by cybercriminals.

Cyberterrorists choose vulnerable targets for IW. Their argument is that they hack for patriotic and political reasons. When hacking takes place supposedly for one of these reasons, it raises a number of tricky issues – should the impacted country hack back or should the hacker be sued? Cybercrimes do not know rational boundaries shown in Fig. 10.8. How do we know the hacker is a patriotic hacker? Should the impacted country declare a war? There are other issues as well – while hacking is illegal, government-sponsored hacking occurs almost everyday. For example, as per revelations by Canadian investigators, there is a cyberspy ring based in China and it is specifically targeting India's defense establishment.[8] This is expected to set off a major cybersecurity revamp by New Delhi.

10.6.2 Cyber Jihadist on the Rise

"Cyber jihadists" utilize their computer skills to hack into the servers of key organizations, and use those servers, unknown to the provider, as de facto ISPs or proxy servers. This tactic allows cyber jihadists to post

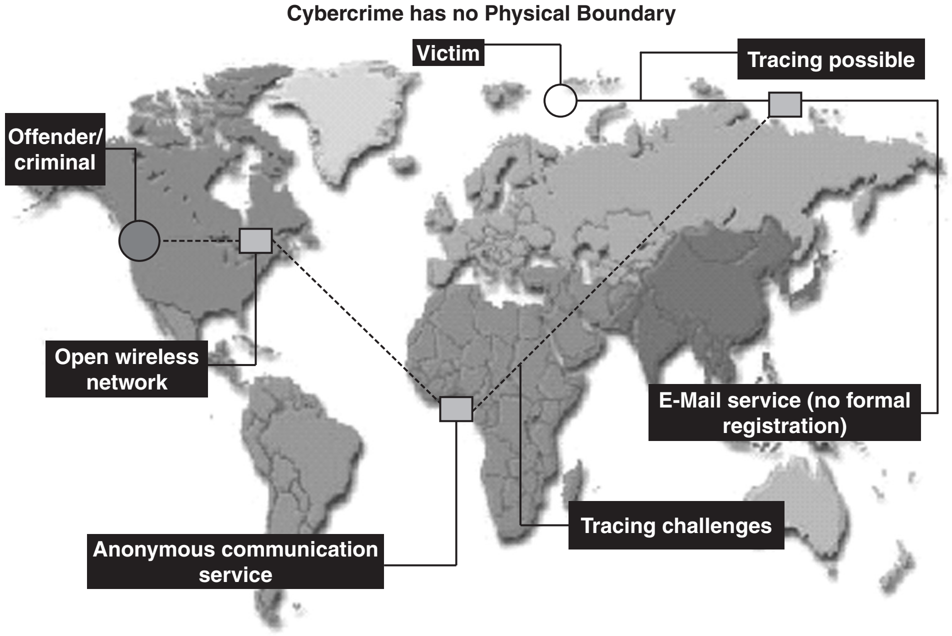
Cybercrime has no Physical Boundary
Victim
Tracing possible
Offender/ criminal
Open wireless network
E-Mail service (no formal registration)
Tracing challenges
Anonymous communication service

Figure 10.8 Cybercrimes are boundary-less!

Box 10.9 Privacy on the Internet and TOR

"Internet privacy" or "online privacy" seem to have become a hot topic! Recently, there is a lot of attention to privacy issues and most seems to be focused on Internet privacy. This may sound strange to some people because consumer-privacy concern did exist long before online business started. The current hype surrounding the Internet, in general, has contributed to the excitement about the topic of Internet privacy. Nowadays, any happening online seems to draw much more attention than the happenings in the "real" world. There is some substance though, behind the hype attached to "Internet privacy." We often reveal a lot of information about ourselves when we go online, information we may not realize we are disclosing, but which advertisers and commercial websites can use to sell us goods and services. "Cookies" have caused a lot of privacy concerns – for details see Box 9.2 (Cookies and Internet Activities) in Chapter 9. Also refer to Chapter 30, Ref. 5, Books, Further Reading.

Much was mentioned about "Information privacy" in Chapter 6 while discussing about the legal perspective and laws around the world. It is worth understanding about Internet privacy. Internet privacy consists of privacy over the media of the Internet: the ability to control what information one reveals about oneself over the Internet, and to control who can access that information. Many people use the term to mean universal Internet privacy: every user of the Internet possesses Internet privacy. Netsukuku is the name of an experimental peer-to-peer routing system, developed by the FreakNet MediaLab (Italian), born to build up a distributed network, anonymous and censorship-free, fully independent but not necessarily separated from Internet, without the support of any server, ISP and no central authority. It does not rely on a backbone router, or on any routing equipment other than normal network interface cards.

Operator YAPO (Yet another Portable Opera) is a portable version of the Opera web browser. It can be installed on portable data storage devices like USB sticks and hard drives. OperaTor only anonymized the following two protocols: HTTP and HTTPS. Other protocols like BitTorrent or the complete part of Opera Mail would not be anonymized.

The Onion Router (TOR), an anonymity network, is a free software descendant of second-generation onion routing enabling Internet anonymity by thwarting network traffic analysis. TOR is a distributed, anonymous network. The network is not run by one organization, but by a diverse set of organizations and individual donating their bandwidth and processing power. The software is open source, so anybody can check for backdoors and other flaws. The project is maintained by the Free Haven Project, and its web resources are donated by the Electronic Frontier Foundation. The name TOR originates as an acronym of "The Onion Routing project." The most common argument against tools for anonymous communication is that criminals can use it to plan future crimes, exchange illegal content, etc. without revealing themselves. The people behind TOR say that while this is true, it should not stop ordinary citizens from communicating anonymously. Criminals already have the means to be anonymous – why should citizens not use anonymous mode of communication to maintain their privacy.

So what are the legitimate reasons for ordinary people to be anonymous there? Common reasons to use TOR are to avoid being tracked by advertising companies on the Web, reach Internet services and sites blocked by the ISP or participating in chat rooms in an anonymous manner. Most people can probably think of at least one reason to be anonymous on the Net without causing anybody else any harm. Government agencies use TOR for intelligence gathering and people in China[9] and other countries without freedom of speech use it to communicate with other freedom seekers.

For a complete reading on privacy, refer to Ref. #5, Books, Further Reading.

their sites and deliver their communications while obscuring their own Internet Protocol address. Other cyber jihad websites rely on the knowledge that ISPs worldwide are not required to monitor content or to control access to sites on their servers until they are made aware of egregious contents on a particular site. Cyberattacks usually react to international events, not vice versa. They could help to spin a delicate diplomatic dance out of control. Hackers from some countries operate independent of each other while hackers from some countries operate as a coordinated pack.

One specific approach that the Indian government might have to consider, relates to what in industry parlance are known as defensive and offensive hackers. While the former's job would be to ensure strong defense against all attacks, that of the latter would be to actively be part of hackers worldwide who perform the role of flooding malware or malicious software codes used to infiltrate large systems. Such participation is crucial to pre-empting attacks. Perhaps, time has come for Indian government to seriously consider creating the position of a cybersecurity czar with the mandate to fundamentally overhaul cybersecurity and bring the currently fragmented networks under a clearly defined structure. Indian government can consider tapping the talents of cybersecurity community constituted by young professionals in their 20s and 30s. Since this community is used to working in a highly non-hierarchical environment with a great deal of personal freedom the government will have to use the office of the cybersecurity czar as its interface with the young professionals.

Summary

In this chapter, we discussed about ethics and morality in the context of cyberspace. We described the mindset of hackers and other cybercriminals as well as their skills, knowledge and competencies. We started the discussion with "Intellectual property." Our IP resides in the cyberspace. As we become "netizens," that is, citizens of cyberspace, we should learn how to be decent individuals. For that a consideration of ethics and the social implications of computing is essential and ideally, it should start at school level. There seems to be little basic understanding of ethical issues. For example, while a large number of people are untouched by IT, there is no provenance for what is published on the Web, so children in particular need to be taught ethical principles to help them differentiate between the useful and ethically good, and the harmful and ethically bad.

We also touched upon the idea of "Information Warfare" which has become possible given the critical role of computers in industry, commerce, government, research, education, medicine, communication systems, entertainment and many other areas of our society. Professional contributors to the design, development, analysis, specification, certification, maintenance, study or myriads of different applications of computer systems exert considerable influence on the ultimate products and services. As such, due to their associative role in this work, these contributors would also have opportunities to both make positive contributions to the society and also to cause harm. Most technology-based products present one or other potential dangers, and thus computer engineering is an intrinsically risky activity.

Today, having the knowledge on hacking is considered useful because hacking is becoming a profession with high fees paid to hackers. There is a huge growth in the number of hackers who attack Web-based systems in particular. Many companies now have on their board paid professional hackers who can test the security of the company website. Globalized cyberattacks will grow and will also improve in sophistication of attack methods and tools used. People on the trailing edge of the digital world also represent a social issue that needs to be considered. Currently many do not even have access to the virtual world, or they may find that they are suffering from de-skilling as their jobs are replaced by software tools or assistive technology.

To ensure that their efforts will be used for good, computing professionals must commit themselves to making computing beneficial and respected profession, promoting an ethical approach to the professional practice. There is a need for increase in the general public awareness on ethical aspects of technology. The domain of cybercrimes has attracted a lot of media attention; it is a high media attention zone. However, in any form of work in the cyberspace, understanding, awareness and appreciation of ethical, social and political dimension involved, are essential.

Review Questions

1. What is meant by "ethics" and "morality"? Is there any relation between these two terms?
2. What is an "IP"? What are the different forms of "intellectual property" mentioned in the chapter?
3. Explain the difference between Trade Name and Trade Secret.
4. What is cybersquatting? Explain how cybersquatting is related to domain name.
5. In the cyberspace and E-Commerce world, what are the new emerging threats to people's intellectual property? Explain with suitable illustration.
6. How do you see the convergence of technologies possibly creating nuisance to innocent individuals? You can provide an example to illustrate your point.
7. Briefly describe the "generations" of hackers along with key characteristics of each generation
8. Mini Assignments.

   (a) Suppose, after completing your Computer Engineering degree, as a computer graduate you decide to enter the professional domain. You start working as a programmer for business software. Soon you notice that the team that you are part of is aware of defects in the software that they have designed to optimize purchase orders. In certain situations the software calculates higher purchases than necessary. The result is that the client ends up spending more money than necessary. However, these defects are hidden, because the team does not have the time to improve the software and a defect would have to be repaired without charge. You also notice that in the organization where you are working with this team there is an implicit agreement to do nothing as long as the client does not notice (this is very improbable due to the number crunching nature of the software). The other programmers in your team and team managers argue that code always contains bugs and that the damage produced is only marginal. What is your view point? Explain with appropriate arguments.

   (b) Your niece is a freshly graduated computer professional and she just started working for a middle-sized software company. She has the impression that the software that she contributes to is quite complicated and lacks usability. There are no specialists within the company on these topics; so she decides to seek outside help. However, the management tries to talk to her about this. She finds that no one seems to regard usability as a relevant topic in the organization. Her graduate thesis involved software usability as the topic and therefore she feels she has some intuitive understanding of it. Other doubts she develops is the quality of a user manual. When she mentions her doubts, her colleagues and superiors tell her: "The users will quickly learn to handle this" and "In practice, it is not a problem." What would you advice your young niece? In your view, is she wasting too much time and energy on "user manuals"? Are they necessary?

   (c) A software development division is mandated to develop a software application according to specification. The specification was provided by an IT consultancy. The contact at the client side is provided by its IT unit, which knows the formal workflows, but little details of the concrete use context. The client does not want the user department to be contacted, as it is busy with critical work. It is further argued that the consultancy already performed a task and business process analysis informing the specification. Yet the programmers think that the specification is incomplete and ambiguous. There are many open questions and alternative options regarding concrete implementation details, alternatives in workflows and exception handling. Nevertheless, the end-user department is shielded off. As their company is under pressure to fulfill the contract, the software developers have to proceed according to specifications and to resolve open questions by imagination and replicating solutions from previous projects. Provide your comments on these circumstances.

(**d**) An IT consultant works for a company engaged in providing outsourcing facilities for computing centers. He also consults clients on how to do this. The company makes most of its profits from the provision of outsourcing, and it is the IT consultant's job to convince potential customers to outsource parts of their computing. However sometimes the consultant has the impression that the clients would be better off by keeping these resources and skilled people in-house. Sometimes the consult tries to hint customers at the disadvantages, however, he cannot say this openly, in order to hide his "disloyal" behavior from colleagues or supervisors. Do you feel that the IT Consultant is doing anything wrong? How would you approach the situation if you were the IT consultant?

References

[1] To understand what an IP address is, you can read the explanatory note in the following link: http://www.host.co.in/knowledgebase/tag/class-c-ip-address (23 October 2010).

[2] See this link about *How to Hack a Facebook Account* http://hackyourlove.com/articles/category/catch-a-cheater/ (17 October 2010).

[3] Basic motive for web attacks is profit as shown by the survey mentioned at http://www.breachbytes.com/2008/02/10/breach-security-labs-finds-67-of-web-attacks-motivated-by-profit/ (20 October 2010).

[4] Read about the Brainvisa case at http://www.expressindia.com/latest-news/brainvisa-discusses-its-rs-47-crore-fraud-case-at-cyber-workshop-to-help-others-learn/408545/ (1 September 2010).

[5] The National Defense Research Institute's report titled *Strategic Information Warfare: A New Face of War* by Molander, R.C., Riddile, A.S. and Wilson, P.A. can be read at: http://www.rand.org/pubs/monograph_reports/MR661/MR661.pdf (17 October 2010).

[6] A study *Self-reported Computer Criminal Behavior: A Psychological Analysis* by Rogers, M., Seigfried, K. and Tidke, K. at the Purdue University Cyberforensics Lab can be read at: http://www.forensics.nl/presentations (25 October 2009).

[7] Below are the links about *Cyber Jihad*
http://www.globaljihad.net/view_page.asp?id=399 (19 October 2010).
http://blogs.csoonline.com/cyber_jihad_cyber_firesale (19 October 2010).
http://www.menassat.com/?q=en/news-articles/3966-islamic-jihad-s-cyber-war-brigades (19 October 2010).
http://ddanchev.blogspot.com/2007/12/cyber-jihadist-hacking-teams.html (19 October 2010).
http://ddanchev.blogspot.com/2007/08/analyses-of-cyber-jihadist-forums-and.html (19 October 2010).

[8] Regarding Cyberspy ring based in China targeting Indian defense establishments (mentioned at the end of Section 10.6.1), refer to the following links:
http://www.financialexpress.com/news/chinalinked-cyber-spy-ring-targeting-india-finds-report/600963/ (2 March 2011). China-linked Cyberspy ring targeting India report.
http://defenceforumindia.com/showthread.php?t=9397&page=2 (2 March 2011). China hacking into Indian Defense Ministry.
http://www.impactlab.net/2010/05/05/china-cyber-spying-network-targeting-india/ (2 March 2011). China Cyber-Spying Network Targetting India.

[9] A 2009 report prepared by US-China Economic and Security Review Commission titled *Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation* is available at: http://www.uscc.gov/researchpapers/2009/NorthropGrumman_PRC_Cyber_Paper_FINAL_Approved%20Report_16Oct2009.pdf (17 October 2010).

Further Reading

Additional Useful Web References

1. India does not have adequate supply of Ethical Hacker. Read an article in Economic Times at: http://economictimes.indiatimes.com/infotech/internet/Supply-of-ethical-hackers-in-India-short-of-demand/articleshow/5238100.cms (16 October 2010).
2. Read article *Mind of a Russian Hacker* in the following links:
   http://certcollection.org/forum/topic/22766-inside-the-mind-of-a-russian-hacker/ (17 October 2010).
   http://www.brightonwired.co.uk/news.php/43895-Inside-the-mind-of-a-Russian-hacker (17 October 2010).
3. More articles about the mind of a hacker are available in the following links:
   http://www.csoonline.com/article/219654/inside-the-hacker-s-mind (16 October 2010).
   http://www.eweek.com/c/a/Security/Inside-the-Mind-of-a-Hacker-[2]/1/ (16 October 2010).
4. What goes on inside the head of a hacker? Read an interesting article at: http://www.csisite.net/LawOfficerArticle.pdf (16 October 2010).
5. There is an article *An Exploration of Cyberspace Security R&D Investment Strategies for DARPA* at: http://www.rand.org/pubs/monograph_reports/MR797/ (1 September 2010).
6. Internet censorship is control or suppression of the publishing or accessing of information on the Internet. The legal issues are similar to offline censorship. Visit some useful links at:
   http://en.wikipedia.org/wiki/Internet_censorship (12 October 2010).
   http://computer.howstuffworks.com/internet-censorship.htm (12 October 2010).
   http://www.siliconindia.com/shownews/Internet_censorship_coming_to_India_-nid-57075.html (12 October 2010).
   http://www.ketan.net/INTERNET_CENSORSHIP_IN_INDIA.html (12 October 2010).
7. Read article bypassing Internet censorship at:
   http://www.nogw.com/download/2005_bypass_censor.pdf (1 October 2010).
   http://www.scribd.com/doc/12714224/how-to-bypass-internet-censorship (1 October 2010).
   http://www.masternewmedia.org/privacy_security/bypass-internet-censorship/bypass-internet-filters-anonymous-browsing-guide-20071118.htm (1 October 2010).
   http://labnol.blogspot.com/2006/07/bypass-internet-censorship-how-to.html (1 October 2010).
   http://infoteknotainment.com/bypass-firewalls-bypassinternet-censorship-with-freegate (1 October 2010).
8. Some more links on the topic of *Internet Censorship* are available at:
   To know more about Internet Censorship FAQs, visit: http://www.spectacle.org/freespch/faq.html (12 October 2010).
   To know more about Internet Censorship – Law and Policies around the world, visit:
   http://www.efa.org.au/Issues/Censor/cens3.html (12 October 2010).
   To know more about Internet Censorship today, visit: http://censorship.suite101.com/article.cfm/internet_censorship_today (12 October 2010).
   To know more about Internet Censorship in Pakistan, visit: http://thecurrentaffairs.com/wikipedia-org-blocked-in-pakistan-internet-censorship-in-pakistan.html (12 October 2010).
   To know more about Internet Censorship in China, visit: http://wapedia.mobi/en/Internet_censorship_in_mainland_China (12 October 2010).
9. Visit the following link where warning about hacking into your spouse's or partner's E-Mail account is mentioned: http://www.experienceproject.com/stories/Had-An-Online-Affair/695263 (15 October 2010).

10. The following link is about *Relationships spoilt by the Internet*: http://www.oddee.com/item_97154.aspx (15 October 2010).
11. Read another interesting story *Pune techies who turned hackers for divorce, alimony* at: http://www.ndtv.com/article/cities/pune-techies-turn-hackers-for-divorce-alimony-47294 (12 October 2010).
12. Some free tools to bypass firewalls and access blocked websites are mentioned at:
    http://www.sizlopedia.com/2008/03/14/10-free-tools-to-bypass-firewalls-and-access-blocked-websites/ (14 October 2010).
    http://www.peacefire.org/info/blocking-software-faq.html (14 October 2010).
13. To read article *Privacy Protection: Time to Think and Act Locally and Globally* by Esther Dyson, visit http://131.193.153.231/www/issues/issue3_6/dyson/index.html (24 December 2010).
14. Another article *Rising Privacy Concerns about Internet* is mentioned in the following link: http://www.msnbc.msn.com/id/22685515/ns/technology_and_science-security/ (16 October 2010).
15. Read article *Mobile Internet Privacy Concerns* at: http://www.euractiv.com/en/infosociety/regulator-warns-mobile-internet-privacy-concerns/article-172783 (17 October 2010).
16. Inspiring story of a 13-year-old ethical hacker is posted at: http://changeminds.wordpress.com/2009/12/21/inspiring-story-of-13-yr-old-ethical-hacker/ (14 October 2010).
17. Read article *Opinion Poll about the Question Whether Knowledge about Hacking is Good or Bad*, visit: http://toostep.com/debate/hacking (19th October 2010).

Books

1. Godbole, N. (2009) *Information Systems Security: Security Management, Metrics, Frameworks and Best Practices* (Chapter 38), Wiley India, New Delhi.
2. Ibid – Chapter 38 (Section 38.13 *Understanding Intellectual Property and its Various Forms*).
3. Ibid – Chapter 31 (Section 31.2 *Privacy Implications of RFID Technology*).
4. Ibid – Appendix AI (*Cybercrime and Information Security*).
5. Ibid – Chapter 29–32 (various dimensions of "Privacy" and related dimensions).
6. Denning, D.E. (1998) *Information Warfare and Security*, Addison–Wesley.
7. Libicki, M.C., *Conquest in Cyberspace: National Security and Information Warfare*, Cambridge University Press, NY.
8. Parker, T. *et al.* (2004) *Cyber Adversary Characterization: Auditing the Hacker Mind*, Syngress Publishing Inc., MA, USA.

Articles and Research Papers

1. Vinod Anand's paper *Chinese Concepts and Capabilities of Information Warfare* can be read at: http://www.idsa.in/system/files/strategicanalysis_vanand_1206.pdf (15 October 2010).
2. Articles on the topic of Information Warfare can be read at:
   http://acorn.nationalinterest.in/tag/information-warfare/ (10 October 2010).
   A PCQuest Article on the topic "Information Warfare" by Ashish Sharma is available at:
   http://pcquest.ciol.com/content/technology/102101206.asp (10 October 2010).
   India Forum for a discussion on *India's Offensive Cyber Warfare* can be visited at:
   http://www.india-forum.com/forums/index.php?/topic/2465-cyber-warfare/ (15 October 2010).
3. The IIT Delhi presentation on *Information Warfare: Challenges of a National Defensive Strategy* is available at: http://www.iimahd.ernet.in/sim09/Speakers/MrMMChaturvedi2.pdf (1 August 2010).
4. To read article about *Cyber Terrorism: World Wide Weaponisation!* by Amaresh Pujari, IPS Inspector general of police (Training), Tamilnadu Police, Chennai, visit http://cii.in/WebCMS/Upload/Amaresh%20Pujari,%20IPS548.pdf (18 October 2010).

5. "Free software" is a matter of liberty, not price – To understand the concept read article in the following link: http://www.gnu.org/philosophy/free-sw.html (19 October 2010).
6. *Ethical Implications of Modifying Modern Mobile Computing Platforms* – the 2009 paper by Juston Western from Auburn University is available at: http://www.justonwestern.com/auburn/MobileComputingEthics.pdf (17 July 2010).

Video Clips

1. Visit a video clip that explains the *Difference between Hackers and Cyber Criminals* at: http://www.youtube.com/watch?v=w0u_7DHuuNg (20 October 2010).
2. A video clip about life of a hacker is available at: http://www.youtube.com/watch?v=ctEUFYELOL0 (24 December 2010).
3. Another video clip about hacker is mentioned in the following link: http://www.youtube.com/watch?v=8D2iU8wD_tk&NR=1&feature=fvwp (16 October 2010).
4. Links to video clips in Box 10.9 (Privacy on the Internet) are quoted in the following link:
   http://video.google.com/videoplay?docid=4938974944926079757# (16 October 2010).
   http://www.youtube.com/watch?v=CrW4FC0OVOQ (16 October 2010).
5. In the following link there is a video clip to educate you about *protecting against Cyber Squatting*. The clip can be seen in reference to discussion in Section 10.2.6 and Box 10.3 in the chapter.
   http://www.youtube.com/watch?v=Y0rbFA71Mkw&feature=related (22 March 2010).
   In the following link there is a video clip titled *Have you ever been Cybersquatted*:
   http://www.youtube.com/watch?v=PoKoiJkQO4E&feature=related (22 March 2010).

The appendices that serve as extended material for the topic addressed in this chapter are: A, B, C, D, F, L, N, R, S, T. They are provided in the companion CD.