Cybercrimes and Cybercriminals

- Stories involving computer crime have been highly publicized in the media.
- The media has often described computer criminals as “hackers.”
- The media also sometimes portrayed hackers in the early days of computing as “heroes.”
- The public’s attitude toward computer crimes has evolved, mainly because of our increased dependency on the Internet.
A "Typical" Cybercriminal

- Some think of a typical computer criminal as a person who is a very bright, technically sophisticated, young male.

- Parker (1998) distinguishes between “hackers” (as nonprofessional or “amateur” criminals) and professional criminals.
Parker claims that computer hackers, unlike most professional criminals, tend:

- Not to be motivated by greed;
- To enjoy the “sport of joyriding.”

He describes “typical computer hackers” as exhibiting three common traits:

1. precociousness;
2. curiosity;
3. persistence.
• Forester and Morrison (1994) note that typical computer criminals can be:
  Ø (amateur) teenage hackers;
  Ø professional criminals;
  Ø (formerly) loyal employees who are unable to resist a criminal opportunity presented by cybertechnology.
The Evolution of “Hacker”

• Himanen (2001) notes that the term “hacker” originally applied to anyone who:
  – "programmed enthusiastically";
  – believed that “information sharing is a powerful positive good.”

• The term “hacker” now has a negative connotation.
Himanen also notes that a hacker need not be a computer enthusiast.

A hacker, in the original sense of the term, could be an “expert or enthusiast of any kind.”

Example:
   someone can be an astronomy hacker.

Hackers are now sometimes also distinguished from “crackers.”
Hackers vs. Crackers (Continued)

- The *Hacker Jargon File* defines a "cracker" as one “who breaks security on a system.”

- Unlike many traditional hackers, crackers typically engage in acts of theft and vandalism, once they gain access to a computer.
Some use the expressions *white hat hacker* and *black hat hacker* (see for example, Wall 2007) to distinguish between the two types of behavior separating hackers from crackers.

- “White hat hackers" are described as engaging in “non-malicious” forms of hacking.

- “Black hat hackers" are viewed as engaging in behavior that is described above as "cracking."
Simpson (2006) notes that many malicious hackers do not possess outstanding technical skills, but they nevertheless know how to locate sophisticated “hacking tools” that can be downloaded from the Internet for free.

Many of these individuals also know how to take advantage of “holes” in computer systems.

Some programmers refer to these “hackers” as “script kiddies” or “packet monkeys,” since they copy code from knowledgeable programmers as opposed to creating the code themselves.
Counter Hacking or “Hacking Back” (Active Defense Hacking)

- Can counter hacking or “hacking back” (at hackers) be justified?
- Counter hacking has been done both by individuals and corporations.
- Counter-hacking attacks are typically directed against those suspected of originating the hacker attacks.
Counter hacking can be either *preemptive* or *reactive*.

Both forms are controversial, but preemptive counter hacking is more difficult to defend.

Is counter hacking an act of *self-defense*, or is it simply another case of “two wrongs making a right”?
• Because counter hacking can cause harm to innocent individuals, some question whether it can be defended on moral grounds.

• Himma (2008) notes that in cases of hacking back against denial of service (DoS) attacks, many innocent persons are adversely affected because the attacks are routed through their computer systems.
• Hackers can use the computers of innocent persons as “host computers” to initiate their attacks.

• This technique is called “IP spoofing.”

• Victims assume that the attacks originated from the host computer, rather than from the actual computer that initiated the attack.

• So when victims hack back, they can unintentionally cause the intermediate computer to be assaulted by bogus requests for service.
Hacking and the Law

• Can some forms of traditional hacking be viewed as an expression of individual freedoms, defended on Constitutional grounds in the US?

• Some advocates for “hacker’s rights” note that traditional forms of hacking played an important role in computer developments and breakthroughs.

• Some of today’s “computer heroes” (and successful entrepreneurs in the computer industry) engaged in past behavior that could be viewed as forms of hacking behavior (Jordan 2008).
Hacking and the Law (Continued)

- Non-malicious hackers enjoy support from civil liberties organizations and from many in the computer community.

- However, the government and business sectors view hacking activities in any form as an invasive activity.

- Many now see hacking as a form of trespass.

- Current legislation against trespass in cyberspace has taken the side of business, government, and law enforcement agencies.
Criteria for Determining Computer Crimes

- When is a crime a *computer crime*?
- There is often a problem of clear *criteria*.

For example, are all crimes involving either the use or the presence of a computer necessarily computer crimes?

- Gotterbarn (1995) criticizes this view by asking whether a murder committed with a surgeon’s scalpel is an issue for medical ethics or just an ordinary crime.
• Do we need a separate category of computer crime/cybercrime?
• Some crimes have involved technologies, but do not require separate categories of crime.

Examples:
• Consider that people steal televisions, but we don't have a category of television crime.
• They also use automobiles to commit crimes, but we don't have a category of automobile crime.
• Review three hypothetical scenarios (described in the textbook) involving crimes in a computer lab:
  
  - *Scenario 1*: Sandra steals a computer device (e.g., a printer) from a computer lab;
  - *Scenario 2*: Bill breaks into a computer lab and then snoops around;
  - *Scenario 3*: Ed enters a computer lab that he is authorized to use and then places an explosive device, which is set to detonate a short time later, on a computer in the lab.
Each of the acts described in the three scenarios is criminal in nature.

But should any of them be viewed as computer crimes?

One might argue that it would not have been possible to commit any of the three crimes if computer technology had never existed.

But these criminal acts can easily be prosecuted as ordinary crimes involving theft, breaking and entering, and vandalism.
Defining Computer Crime

- Forester and Morrison (1994) define a computer crime as “a criminal act in which a computer is used as the principal tool.”
- This definition rules out the crimes committed in our three (computer-lab-related) scenarios as “computer crimes.”
- But is Forester and Morrison's definition of computer crime adequate?
Towards a Coherent Definition of Cybercrime

- We define a (genuine) cybercrime as a crime in which the criminal act can:
  - be carried out only through the use of cybertechnology, and
  - take place only in the cyber realm.
- Like Forester and Morrison's definition, this one rules out the three scenarios involving the computer lab as genuine cybercrimes.
- And it also rules out the income tax scenario.
Using our definition of cybercrime, we can identify specific cases of genuine cybercrimes.

We can also differentiate three broad categories of (genuine) cybercrime:

1. cyberpiracy,
2. cybertrespass,
3. cybervandalism.
Three Categories of (Genuine) Cybercrime

1. **Cyberpiracy** - using cybertechnology in unauthorized ways to:
   a. reproduce copies of proprietary software and proprietary information, or
   b. distribute proprietary information (in digital form) across a computer network.

2. **Cybertrespass** - using cybertechnology to gain or to exceed unauthorized access to:
   a. an individual's or an organization's computer system, or
   b. a password-protected Web site.

3. **Cybervandalism** - using cybertechnology to unleash one or more programs that:
   a. disrupt the transmission of electronic information across one or more computer networks, including the Internet, or
   b. destroy data resident in a computer or damage a computer system's resources, or both.
Examples of the Three Categories of (Genuine) Cybercrimes

• Consider three actual incidents:
  1) distributing proprietary MP3 files on Napster and related peer-to-peer (P2P) file sharing sites;
  2) unleashing the Conficker Virus;
  3) Launching the denial-of-service (DoS) attacks on commercial Web sites.

• We can use our model of cybercrime to see where each incident would fall.
Categorizing (Genuine) Cybercrimes

• Crimes involving the unauthorized exchange of proprietary MP3 files would come under the category of cyberpiracy (Category I).

• The crime involving the Conficker Virus falls under cybervandalism (Category III).

• The denial-of-service attacks on Web sites falls under the heading of cybertrespass (Category II), as well as under Category (III).
  ➢ Note that this cybercrime spans more than one category, as some cybercrimes can.
Distinguishing Cybercrimes from Cyber-related Crimes

• Many crimes that involve the use of cybertechnology are not *genuine* cybercrimes.

- For example, crimes involving pedophilia, stalking, and pornography can be carried with or without the use of cybertechnology.

- Nothing about these kinds of crimes is unique to, or requires the use of, cybertechnology.

- These crimes are better understood as examples of *cyber-related* crimes.
Cyber-related Crimes

- Cyber-related crimes can be further divided into two sub-categories:
  - cyberexacerbated crimes;
  - cyberassisted crimes.
Cyber-exacerbated vs. Cyber-assisted crimes

• We can also further distinguish between a crime in which cybertechnology is used to:
  (a) file a fraudulent income-tax return,
  (b) stalk people, distribute pornography, solicit minors for sex.

• In (a), a computer assists in a way that is trivial and possibly irrelevant.

• In (b), cybertechnology has played a much more significant (i.e., an exacerbating) role.
Crimes Involving Cybertechnology

• Crimes involving cybertechnology can be classified in one of three ways:
  ➢ Cyberspecific crimes (i.e., *genuine cybercrimes*);
  ➢ Cyberexacerbated crimes;
  ➢ Cyberassisted crimes.
Figure 7-1: Cybercrimes and Cyber-related Crimes

**Cybercrimes**
- Cyberspecific
  - Cyberpiracy
  - Cybertrespass
  - Cybervandalism

**Cyberrelated Crimes**
- Cyberexacerbated
  - Cyberstalking
  - Internet Pedophilia
  - Internet Pornography
- Cyberassisted
  - Income-tax cheating (with a computer)
  - Physical assault with a computer
  - Property damage using a computer hardware device (e.g., throwing a hardware device through a window)
Identity Theft: A Cyber-related Crime

- Identity Theft would qualify as an example of a cyber-exacerbated crime
- Lininger and Vines (2005) define identity theft as:
  
  a crime in which an imposter obtains key pieces of personal information, such as Social Security or driver’s license numbers, in order to impersonate someone else.

- They go on to note that the information can be used to obtain credit, merchandise, and services in the name of the victim, or to provide the thief with false credentials.
• Identity-theft crimes can also include the taking of another person’s identity through the fraudulent acquisition of personal information in credit card numbers.

• Wall (2007) notes that identity theft is often mistakenly used to describe crimes involving credit card theft.

• So, not all instances of the latter kind of theft qualify as identity theft.
Identity theft, like other cyber-related crimes, does not require cybertechnology.

Consider that in the past, identity thieves have combed through dumpsters looking for statements containing account information on credit card bills that people dispose of in their trash (commonly referred to as “dumpster diving”).

Identity thieves have been very successful in scams involving cybertechnology in general (e.g. in recording credit card “swipes”), independent of the Internet per se.
Simon (2005) notes that factors such as “lax security” and “carelessness involving computer databases” has made it easy for some identity thieves to acquire personal information about their victims via the use of cybertechnology.

Two examples that occurred in 2005:
- **Bank of America** lost computer tapes containing data on 1.2 million federal employees;
- **ChoicePoint**, Inc. and Lexis-Nexis disclosed that the dossiers of more than 170,000 Americans on the companies’ databases had been illegally accessed by criminals, and that at least 750 of them had their identities stolen.
• Simon (2005) also notes that the information in these databases contained the addresses and social security numbers of individuals.
  ➢ For example, all the information that identity thieves needed to open up a credit card account.

• Simon points out that another incident linked to lax security and carelessness involved an MCI laptop computer containing the names of 165,000 current and former MCI employees.
  ➢ The computer was stolen from the car of an MCI analyst, which was parked in front of the analyst’s home garage.
Identity Theft as a Cyber-related Crime (Continued)

• Many kinds of identity-theft scams have been carried out on the Internet.
• One common example is a scheme involving email that appears to be from a reputable business.  
  ➢ For example, you may receive email that looks like it was sent by eBay, Amazon, or PayPal.
• The emails often look legitimate because they include the official logos of the companies they claim to be.
• Some messages inform you that your account is about to expire and that you need to update it by verifying your credit card number.
Identity Theft as a Cyber-related Crime (Continued)

How can a potential victim differentiate legitimate email sent from businesses like eBay or PayPal from that sent by identity thieves?
• Typically, email from identity thieves will not address the potential victim by name.
• This often indicates that the e-mail is not from a legitimate source.
• Many emails sent from identity thieves are generated through spam via a technique referred to as “phishing.”
Technologies and Tools Used to Combat International Cybercrime

• Two kinds of tools/technologies that have been used to fight cybercrime at the international level are:
  – *Biometrics*;
  – *Keystroke monitoring*
Biometrics Technologies

• *Biometrics* can be defined as:
  
  the biological identification of a person, which includes eyes, voice, hand
  prints, finger prints, retina patterns, and handwritten signatures (Power,
  2000).

• van der Ploeg (2004) notes that with biometrics tools, a person’s:
  
  ➢ iris can be “read” in the same way that a person’s voice can be printed.
  ➢ fingerprints can be “read” by a computer that is “touch sensitive” and “endowed with hearing
    and seeing capacities.”
Biometrics Technologies (Continued)

- In 2002, an iris-scanning device, which is a type of biometric identification scheme, was first tested at London's Heathrow Airport.

- These kinds of scanning devices capture a digital image of one's iris, which is then stored in a database.

- The digital image can be matched against images of individuals, including those entering and leaving public places.
Biometrics Technologies: Facial-Recognition Programs in the U.S.

- At Super Bowl XXXV in January 2001, face-recognition technology was used by law-enforcement agencies to scan the faces of persons entering the football stadium.

- The scanned images were instantly matched against electronic images (faces) of suspected criminals and terrorists, contained in a central computer database.

- Initially, this was controversial; after September 11, 2001, it was widely supported.
Keystroke Monitoring Software

- Law-enforcement agencies have used a technology called *keystroke monitoring* to track down professional criminals.
- Keystroke-monitoring software records every key struck by a user, as well as every character of the response that the system returns to the user.
Keystroke Monitoring (Continued)

• Keystroke-monitoring software can trace the text in electronic messages back to the original sequence of keys and characters entered at a user's computer keyboard.
• It is especially useful in tracking the activities of criminals who use encryption to encode their messages.