Among the questions examined in this chapter are:

- What is cybercrime, and how can it be distinguished from cyber-related crimes?
- Can a meaningful distinction be drawn between hacking and "cracking" in the context of cybertechnology?
- What is "active defense hacking" or counter hacking, and is it morally permissible?
- Can biometric technologies be used to assist law enforcement groups in identifying criminals in ways that are ethically permissible?
- Why are jurisdictional issues problematic for prosecuting some cybercrimes?

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.

Defining Computer Crime (Continued)

- Review Scenario 4, where a person ("Sheila") uses a computer to file a fraudulent income-tax return.
- Arguably, a computer is the *principal tool* used by Sheila to carry out the criminal act.
- Has Sheila committed a *computer crime*?
  - Consider that she could have committed the same crime by manually filling out a standard (hardcopy) version of the income-tax forms by using a pencil or pen.

Towards a Coherent Definition of Cybercrime

- We define a (genuine) cybercrime as a crime in which *the criminal act can:*

1) *be carried out only through the use of cybertechnology, and*
2) *take place only in the cyber realm.*

- This definition rules out the three scenarios involving the computer lab as genuine cybercrimes.
- And it also rules out the income tax scenario (scenario 4).

Examples of the 3 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.

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.”

Patriot Act (continued)

- In December 2005, it was reported that the Bush Administration had been monitoring the e-mails and phone calls of U.S. citizens who were communicating with individuals outside the U.S.
- Opponents argued that the Bush Administration's practices violated the law because no court order was requested in conducting surveillance on U.S. citizens.
- It is legal for the National Security Agency (NSA) to conduct wiretaps on non-U.S. citizens, but the NSA is not authorized to intercept the communications of Americans without first getting a court order.

Bush administration argued that it was acting within the law because its primary obligation was to protect the American public against terrorist attack.