Computer Crimes

Hacking Activities

- Some hacking activities can be viewed as examples of three of the principles included in Levy's "Hacker Ethic":

1) information should be (totally) free;
2) hackers provide society with a useful and important service;
3) activities in cyberspace are virtual in nature; so they do not cause real harm to people in the real (physical) world.

“Information Wants to Be Free”

- Should all information be totally free?
- The view that information should be free is regarded by some critics (for example, Spafford 2004) as naïve, idealistic, or romantic.
- Spafford notes that if information were free:
- privacy would not be possible because we would not be able to control how information about us was collected and used.
- it would not be possible to ensure integrity and accuracy of that information.

Do Hackers Really Provide an Important Service?

- Spafford also provides counterexamples to this version of the “hacker argument.”
- He asks whether we would permit someone to start a fire in a crowded shopping mall in order to expose the fact that the mall's sprinkler system was not adequate.
- Alternatively, would you be willing to thank a burglar who successfully broke into your house?
  - For example, would you thank that burglar for showing that your home security system was inadequate?

Does Hacking Causes Only Virtual Harm, Not Real Harm?

- Some argue that break-ins and vandalism in cyberspace cause no “real harm” to persons because they are activities that occur only in the *virtual realm*.
- This argument commits a logical fallacy by confusing the connection between the real and the virtual regarding harm by reasoning in the following way:
  - *The virtual world in not the real (physical) world; so any harms that occur in the virtual world are not real harms.* (James Moor calls this the *Virtuality Fallacy*.)
- See Chapter 3 for a description of why the reasoning process used in the Virtuality Fallacy is fallacious.

Can Computer Break-ins Ever Be Ethically Justified?

- Spafford suggests that in certain extreme cases, breaking into a computer could be the "right thing to do."
- For example,, breaking into a computer to get medical records to save one’s life.
- However, Spafford also argues that computer break-ins always cause harm.

Ethically Justifying a Computer Break-in (Continued)

- Spafford seems to use a deontological (or non-consequentialist) argument to justify the break-in the case of the medical emergency.
  - For example, Spafford believes that morality is determined by *actions not results*.
- He argues that we cannot evaluate morality based on consequences or results because we would not "know the full scope of those results," which are based on the "sum total of all future effect."
- Spafford's argument tends to be based on a version of *act deontology* (see Chapter 2).

Cyberterrorism

- Dorothy Denning (2004, 2007) defines *cyberterrorism* as the "convergence of cyberspace and terrorism."
- Cyberterrorism covers a range of politically motivated hacking operations intended to cause grave harm that can result in either loss of life or severe economic loss, or both.
- In some cases, it is difficult to separate acts of cyberterrorism from cybervandalism and cyberwarfare, and acts of ordinary hacking.

Cyberterrorism vs. Hacktivism

- *Denial-of-service* (DoS) attacks have been launched for the purpose of preventing users from accessing targeted commercial Web sites.
- These attacks have also resulted in severe economic loss for major corporations.
- Should these DoS-related attacks necessarily be classified as instances of cyberterrorism?
- Or, can some of these attacks be better understood as another form of malicious hacking – i.e., those perpetrated by persons or groups with a particular political agenda or ideology?

Hacktivism

- Manion and Goodrum (2004) have questioned whether some DoS (and related) cyberattacks might be better understood as instances of *hacktivism*.
- For example, they note the outrage on the part of some hackers and political activists that arose because of increasingly the "commodified Internet,“ beginning in the late 1990s.
- They also question whether the behavior of these persons and groups suggests a new form of civil disobedience, which they describe as *hacktivism*.

Can Hacktivism be Justified?

- Himma (2007) describes the line of reasoning that hacktivists and their supporters tend to use to justify their activities as forms of political activism and "electronic civil disobedience" (or ECD):
  - **PREMISE 1.** Because civil disobedience is justifiable as a protest against injustice, it is permissible to commit digital intrusions as a means of protesting injustice.
  - **PREMISE 2.** In so far as it is permissible to stage a sit-in in a commercial or governmental building to protest, say laws that violate human rights, it is permissible to intrude on commercial or government networks to protest such laws.
  - **CONCLUSION.** Digital intrusions that would otherwise be morally objectionable are morally permissible if they are politically motivated acts of electronic civil disobedience, or hacktivism.

Hactivism as a form of Electronic Civil Disobedience (ECD)

- With regard to ECD, Manion and Goodrum (2004) claim that for an act to qualify as "civilly disobedient," it must satisfy the following conditions:
- No damage done to persons or property;
- Nonviolent;
- Not for personal profit;
- Ethical motivation – the strong conviction that a law is unjust, or unfair, to the extreme detriment of the common good;
- Willingness to accept personal responsibility for the outcome of actions.

Hacktivism as a form of ECD (Continued)

- Denning (2008) argues that Manion and Goodrum's analysis of hacktivism suggests that some acts of Web defacement may also be morally justified as ECD, in so far as they are "ethically motivated."
- But Denning points out that defacing a Web site seems to be incompatible with Manion and Goodrum's first condition for ECD – i.e., "no damage."
- ➢ For example, she notes that defacements can "cause information property damage that is analogous to physical property damage" and both can "require resources to repair."

Hacktivism vs. Cyberterrorism

- Can a meaningful distinction be drawn between hacktivism and cyberterrorism?
- Denning (2001) attempts to draw some critical distinctions among three related notions:
- *activism*;
- *hacktivism*;
- *cyberterrorism.*

Activism, Hacktivism, and Cyberterrorism

- *Activism* includes the normal, non-disruptive use of the Internet to support a cause.
  - For example, an activist could use the Internet to discuss issues, form coalitions, and plan and coordinate activities.
- Activists could engage in a range of activities from browsing the Web to sending e-mail, posting material to a Web site, constructing a Web site dedicated to their political cause or causes, and so forth.

Activism, Hacktivism, and Cyberterrorism (continued)

- Hacktivism is the *convergence of activism and computer hacking.*
- It uses hacking techniques against a target Internet site with intent to disrupt normal operations, but without intending to cause serious damage.
- These disruptions could be caused by "e-mail bombs" and "low grade" viruses that cause only minimal disruption, and would not result in severe economic damage or loss of life.

Activism, Hacktivism, and Cyberterrorism (continued)

- Cyberterorism consists of operations that are intended to cause great harm such as loss of life or severe economic damage, or both.
- For example, a cyberterrorist might attempt to bring down the U.S. stock market or take control of a transportation unit in order to cause trains to crash.
- Denning believes that conceptual distinctions can be used to differentiate various activities included under the headings of activism, hacktivism, and cyberterrorism.

Denning’s Analysis

- Denning admits that as we progress from activism to cyberterrorism the boundaries become "fuzzy."
- ➢ For example, should an "e-mail bomb" sent by a hacker who is also a political activist be viewed as hacktivism or as an act of cyberterrorism?
- Many in law-enforcement argue that more effort should be devoted to finding ways to deter and catch these individuals rather than trying to understand their ideological beliefs, goals, and objectives.

Cybertechnology and Terrorist Organizations

- Some members of al Qaeda have fairly sophisticated computer devices, despite the fact that many also operate out of caves in Afghanistan and Pakistan.
- It is not clear that terrorists have used cyber-technology to enhance their activities in ways that this technology could have been used.
- We can ask why terrorists have not yet made more direct use of cybertechnology so far in carrying out specific acts of terror.

Cybertechnology and Terrorism (continued)

- One explanation is that they have not yet gained the expertise with cybertechnology.
- This may change as the next generation of terrorists, who will likely be more skilled in the use of computers and cybertechnology, replace those currently in leadership roles.
- When terrorists flew airplanes into the Twin Towers, on 9/11, they had to take their own lives in the act.
- But suppose that terrorists are someday able to gain control of onboard computer systems on airplanes and override the airplane’s computerized controls.

Cybertechnology and Terrorism (continued)

- Denning (2007) notes that there is evidence that terrorists groups and "jihadists" are interested in conducting cyberattacks, and that these terrorist groups have at least some capability to carry out such attacks.
  - For example, she notes that they are undergoing online training on how to develop the necessary skills.
- But Denning also points out that there is no evidence to suggest either that the threat of cyberattacks from these terrorist groups is imminent or that they have acquired the knowledge or the skills to conduct "highly damaging attacks against critical infrastructure."

Cybertechnology and Terrorism (continued)

- Denning (2008) also notes that there are “indicators” showing that these terrorist groups have an interest in acquiring the relevant knowledge and skills.
- In 2009, the Obama administration created a new post for a Cyber Security Coordinator, mainly in response to threats of cyber attacks from terrorists groups.

Information Warfare

- Denning (1999) defines *information warfare* (IW) as "operations that target or exploit information media in order to win some objective over an adversary."
- Certain aspects of cyberterrorism also seem to conform to Denning's definition of IW, but IW is a broader concept than cyberterrorism.
  - For example, IW need not involve loss of life or severe economic loss, even if such results can occur.

Information Warfare (continued)

- IW, unlike conventional or physical warfare, tends to be *more disruptive than destructive*.
- The instruments of war in IW typically strike at a nation's infrastructure.
- The kinds of "weapons" used typically consist of viruses, worms, and DoS attacks (described earlier).
- The disruption caused by viruses, worms, and DoS attacks can be more damaging, in many respects, than physical damage caused to a nation by conventional weapons.

Information Warfare (continued)

- Moor and others note that in the past, warfare was conducted by physical means – e.g., human beings engaged in combat, using weapons such as guns, tanks, and aircraft.
- But during the first Gulf War, in the early 1990s, we saw for the first time the importance of information technology in contemporary warfare strategies.
- Moor notes that the war was won quickly by the multinational coalition because it was able to destroy the Iraqi communications technologies at the outset and thus put the Iraqi army at a severe disadvantage.

Information Warfare (continued)

- In 2009, the government of South Korea accused North Korea of running a cyberwarfare unit that attempted to hack into both U.S. and South Korean military networks to gather confidential information and to disrupt service.
- North Korea was also suspected of launching the DoS attacks that disrupted the Web sites of 27 American and South Korean government agencies as well as commercial Web sites such as the New York Stock Exchange, Nasdaq, and Yahoo's finance section (Shang-Hun and Markoff 2009).

Information Warfare and Requirements for “Just War”

- Some question whether IW can meet the conditions required for “just” warfare (i.e., a “just war”).
- One condition that must be satisfied for a just war to be carried out is that a distinction be made between combatants and noncombatants.
- Many critics worry that in the context of IW, it may not be possible to make this distinction (and other kinds of important distinctions) affecting just-war requirements.
- So, some have concluded that IW can never be justified solely on moral grounds.

Table 6-1: Hacktivism, Cyberterrorism, and Information Warfare

Hacktivism	The convergence of political activism and computer hacking techniques to engage in a new form of civil disobedience.
Cyberterrorism	The convergence of cyber-technology and terrorism for carrying acts of terror in (or via) cyberspace.
Information Warfare	Using information to deceive the enemy; and using conventional warfare tactics to take out an enemy's computer and information systems.

Computer Security and Risk Analysis

- Risk analysis is a methodology used to come to an informed decision about the most cost-effective controls to limit the risks to your assets *vis-à-vis* the spectrum of threats.
- Banks and credit card companies can tolerate a considerable amount of credit risk and fraud because they know how to anticipate loses and price their services accordingly.
- What is an acceptable level of risk in computer systems, and how can we assess it?

Computer Security and Risk Analysis (Continued)

- Schneier (2004) argues that *security is a process, not a product*.
- He also believes that an important element in that process is *risk assessment*.
- Because "anything worth doing requires some risk," Schneier suggests that seeking perfect security would make a system useless.

Risk Analysis (Continued)

- Schneier believes that risk can be understood and assessed in terms of the net result of the impacts of five elements:
  - assets,
  - threats,
  - vulnerabilities,
  - impact,
  - safeguards.

Risk Analysis (Continued)

- Should the results of a decision procedure based on conventional risk analysis be used to determine security policies involving our national infrastructure?
- This can have implications for the safety and well being of millions of people?
- If the private sector is not willing to pay for enhanced security, does the federal government have an obligation to do so?

Risk Assessment (Continued)

- Many of the ethical issues surrounding computer security are not trivial.
- They have implications for public safety that can result in the deaths of significant numbers of persons.
- So, it is not clear that all computer security issues can be understood simply in terms of the risk analysis model advocated by Schneier.

Risk and the "De-perimeterization of Information Security"

- One reason why it is difficult to determine who is responsible for securing cyberspace may have to do with what Pieters and van Cleeff (2009) call the "de-perimeterization of information security."
  - For example, they note that IT systems "span the boundaries of multiple parties" and "cross the security perimeters" that these parties have put in place for themselves.
- As a result, they argue that we can "no longer achieve adequate cybersecurity" by simply building a "digital fence" around a single organization.

Risk and the "De-perimeterization of Information Security" (Continued)

- According to Pieters and van Cleeff, IT security has become de-perimeterized due to the following trends:
  - many organizations now outsource their information-technology processes;
  - many employees expect to be able to work from home;
  - mobile devices make it possible to access data from anywhere;
  - "smart buildings" are being equipped with small microchips that allows for constant communication between buildings and their headquarters.

Risk and the "De-perimeterization of Information Security" (Continued)

- Pieters and van Cleeff note that de-perimeterization leads to "uncertain risk" for IT security.
- They argue that an adequate analysis of security-related risks now requires a "new paradigm" that integrates elements of the *precautionary principle* (described in Chapter 12).
- Pieters and van Cleeff also point out that the precautionary principle is closely related to the legal concept "duty of care" in that it implies that failure to "exercise care" can result in liabilities for damages.