ILLINOIS TECH | College of Computing

ITMM 485 / 585
Dr. Gurram Gopal

Legal and Ethical Issues in Information Technology

1

ILLINOIS TECH | College of Computing

Ch7: Cybercrime and Technology-Facilitated Crime P1: Hackers and Hacking

2

Learning Objectives:

Upon completion of this lesson the students should be able to:

- Define "active defense hacking" or counter hacking, and discuss whether or not it might be morally permissible
- Explain how law enforcement may use biometric technology in identifying criminals and terrorists and discuss the ethical permissibility of these techniques
- Recall and describe the differences between cybercrime and cyber-related crime
- Explain why jurisdictional issues are problematic in prosecution of cybercrime
- Describe journalistic practices used by organizations such as WikiLeaks, and discuss whether these practices are defensible under a free press or are criminal

3

Module Objectives:

Upon completion of this lesson the students should be able to:

- Define "active defense hacking" or counter hacking, and discuss whether or not it might be morally permissible

4

Cybercrimes and Cybercriminals

- Stories involving computer crime have been highly publicized in the media.
- The media has often described computer criminals as "hackers."
- In the 1970s and 1980s, some in the media portrayed computer hackers as "heroes."
- The media's attitude toward computer hacking has since changed, mainly because of our increased dependency on the Internet.

5

A "Typical" Cybercriminal

- Many think of a typical computer criminal as a someone who fits the profile of a very bright, technically sophisticated, young white male.
- Consider, for example, the lead character portrayed in the popular movie *War Games*.
- Parker (1998) distinguishes between "hackers" (as nonprofessional or "amateur" criminals) and professional criminals.

6

A Typical Computer Criminal…

Parker clams 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:

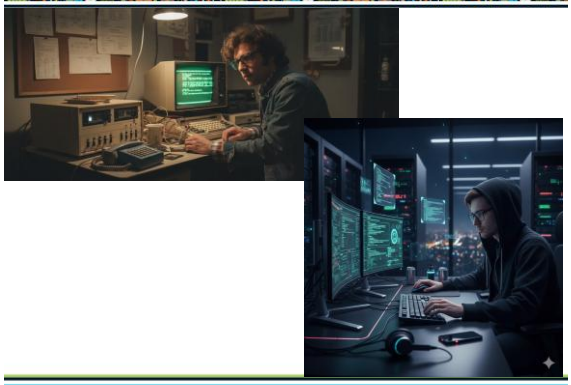
1) precociousness;
2) curiosity;
3) persistence.

7

A Typical Computer Criminal…

- Forester and Morrison (1994) note that typical computer criminals can be:
- (amateur) teenage hackers;
- professional criminals;
- (formerly) loyal employees who are unable to resist a criminal opportunity presented by cybertechnology.

8



9

Hackers vs. Crackers

- The *Hacker Jargon File* defines a "cracker" as one "who breaks security on a system."
- Unlike traditional hackers who enjoy figuring out how to access systems, crackers typically engage in acts of theft and vandalism, once they gain access to a computer.

10

"White Hat" vs. "Black Hat" Hackers

- Others 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."

11

Malicious Hackers and "Hacking Tools" on the Internet

- Simpson (2006) notes that many malicious hackers do not possess outstanding technical skills.
- However, they 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.

12

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.

13

Counter Hacking (Continued)

- 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"?

14

Counter Hacking (Continued)

- 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.

15

Counter Hacking (Continued)

- 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.

16

Certified Ethical Hackers

- What is a *Certified Ethical Hacker*?
- Certified Ethical Hackers (CEH) are trained and *certified* in counter hacking.
- Not only are they trained in the use of defensive measures, but some are also authorized to engage in security-related activities that involve *preemptive* strikes as well.

17

Certified Ethical Hackers (Continued)

- According to the Certified Ethical Hacker (CEH) Web site (www.eccouncil.org/ceh.htm):

  The goal of the ethical hacker is to help the organization take *preemptive measures* against malicious attacks by attacking the system himself; all the while staying within legal limits. [Italics Added]
- The CEH site also states that an

  Ethical Hacker is very similar to a Penetration Tester…When it is done by request and under a contract between an Ethical Hacker and an organization, it is legal.

18

Certified Ethical Hackers (Continued)

- Should it be legal to for Certified Ethical Hackers to engage in preemptive hacking attacks?
- Some who defend preemptive acts of counter hacking believe that they can be justified on utilitarian, or consequentilaist, grounds.
- For example, they argue that less overall harm will likely result if preemptive strikes are allowed.
- However, it would seem that many of the same difficulties that apply to utilitarian arguments (see Chapter 2) would apply here as well.

19

Hacking and the Law

- Can some forms of traditional hacking be viewed as an expression of individual freedoms, defended on Constitutional grounds in the U.S.?
- 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 succes- sful entrepreneurs in the computer industry) engaged in past behavior that could be viewed as forms of hacking behavior (Jordan 2008).

20

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.

21

22