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 P2: Cybercrime & Cyber Related Crime

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:

- Recall and describe the differences between cybercrime and cyber-related crime

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:

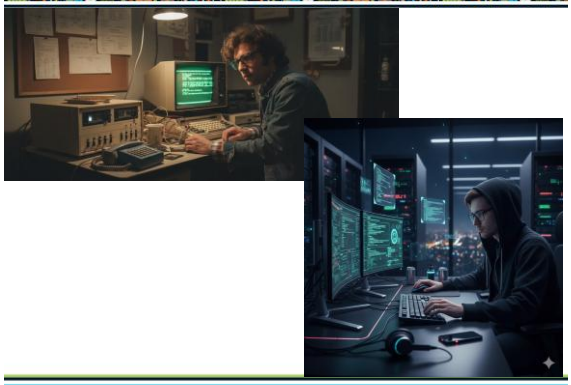
1) precociousness;
2) curiosity;
3) persistence.

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

Criteria for Determining Computer Crimes

- When is a crime a *computer crime*?
- What *criteria* should be used for determining that?
- Some have suggested that all crimes involving either the use or the presence of a computer should count as (examples of) computer crimes.
- But are all of these crimes necessarily computer crimes (and are they issues for computer ethics)?
- Gotterbarn (1995) asks whether a murder committed with a surgeon's scalpel is an issue for medical ethics.
- If not, then why is a crime involving a computer an issue for computer ethics, and why is it a computer crime?

22

Criteria for Determining Computer Crimes…

- Do we need a separate category of computer crime/cybercrime?
- Some crimes have involved technologies, but do not require separate categories of crime.
- 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.

23

Criteria for Determining Computer Crimes…

- Review three hypothetical scenarios (a, b, and c) in the textbook, each describing a crime involving a computer lab:
- *Scenario a*: Sandra steals a computer device (e.g., a printer) from a computer lab;
- *Scenario b*: Bill breaks into a computer lab and then snoops around;
- *Scenario c*: 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 mainframe computer in the lab.

24

Criteria for Determining Computer Crimes...

- 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.

25

Defining Computer Crime

- Robert Moore (2011) suggests that a computer crime can include "any criminal activity involving a compu- ter" (while a cybercrime would include "any criminal activity involving a computer and a network").
- Under Moore's definition, each of the criminal activities described in Scenarios a, b, and c would seem to fall under the category "computer crime."
- However, many would object that Moore's definition of computer crime is far too broad to be helpful.
- So, arguably we need a more precise definition.

26

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*." [Italics Added]
- This definition rules out the criminal acts committed in the three scenarios involving a computer lab as "computer crimes."
- But we can still ask if Forester and Morrison's definition of computer crime is adequate.

27

Defining Computer Crime...

- Review the hypothetical scenario (in the textbook) in which "Sandra" 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.
- So, on Forester and Morrison's definition, Sheila's criminal act might count as *computer crime* .
- But consider the fact that Sheila could have committed the same criminal act by manually filling out a standard (hardcopy) version of the income-tax forms by using a pencil or pen.

28

Defining Computer Crime...

- It would seem that we need an alternative definition.
- Girasa (2002) defines "cybercrime" as

  a generic term covering a multiplicity of crimes found in penal code or in legislation having the "use of computer technology as its central component."
- But what, exactly, is meant by "central component"?
- Was a computer a central component in the scenario where Sheila filed the fraudulent income tax form?
- As in the case of Forester and Morrison's definition, Girasa's does not seem fully adequate.

29

Defining Computer Crime...

- Strickwerda (2013) defines a cybercrime as

  any new or different human act that is carried out through the use of computers or computer networks and is prohibited by the enactment of law.
- Initially, this definition might not seem to be much of an improvement over the earlier definitions that we examined.
- However, Strickwerda's definition does provide an important insight.

30

Defining Computer Crime...

- One virtue of Strikweda's definition is in her insight that a cybercrime is *a new or different human act* (carried out by computers).
- This insight echoes James Moor's point that computers make possible "new kinds of human actions" (as we saw in Chapter 1) and thus generate "policy vacuums" (Moor 2007).
- We incorporate Moor's and Strikwerda's insights in our definition of computer crime.

31

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*

- Unlike the earlier definitions we considered, this one rules out the income-tax scenario as a genuine cybercrime, in addition to ruling out the three scenarios in the computer lab.

32

Genuine Cybercrimes

- 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.

33

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.

34

Examples of the Three Categories of (Genuine) Cybercrimes

- Consider three actual incidents:

1) distributing copyrighted MP3 files (and other proprietary digital content) on illegal file-sharing sites such as The Pirate Bay;
2) unleashing the Heartbleed Virus (2014);
3) launching the Internet-wide denial-of-service attacks on commercial Web sites (2012.

- We can use our model of cybercrime to see where each incident would fall.

35

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 Heartbleed 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 Cybervandalism (Category III). Note that this cybercrime spans more than one category, as some cybercrimes can.

36

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.

37

Cyber-related Crimes

- Cyber-*related* crimes can be further divided into two sub-categories:

i. *cyberexacerbated* crimes;

ii. *cyberassisted* crimes.

38

Cyber-exacerbated vs. Cyber-assisted crimes

- We can also further distinguish between a crime in which cybertechnology is used to:

a) (a) file a fraudulent income-tax return,

b) (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.

39

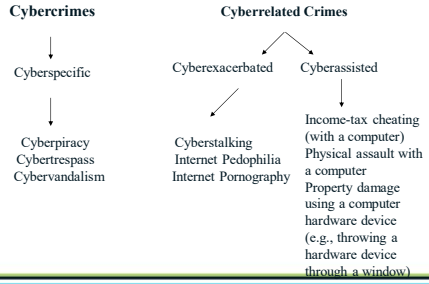
Crimes Involving Cybertechnology

Crimes involving cybertechnology can be classified in one of three ways:

- Cyberspecific crimes (i.e., *genuine cybercrimes*);
- Cyberexacerbated crimes;
- Cyberassisted crimes.

40

Figure 7-1: Cybercrimes and Cyber-related Crimes



41

Identity Theft: A Cyber-related Crime

- In our model, identity theft is a cyber-related crime (that is also 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 some 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.

42

Identity Theft (Continued)

- 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.

43

Identity Theft (Continued)

- 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.

44

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 e-mail 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.

45

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."

46

47