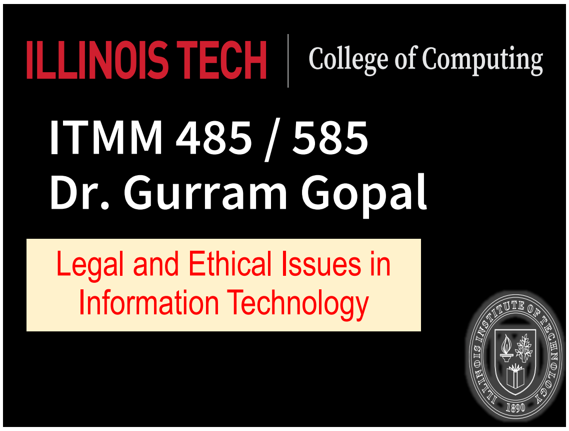


ILLINOIS TECH | College of Computing

ITMM 485 / 585
Dr. Gurram Gopal

Legal and Ethical Issues in Information Technology

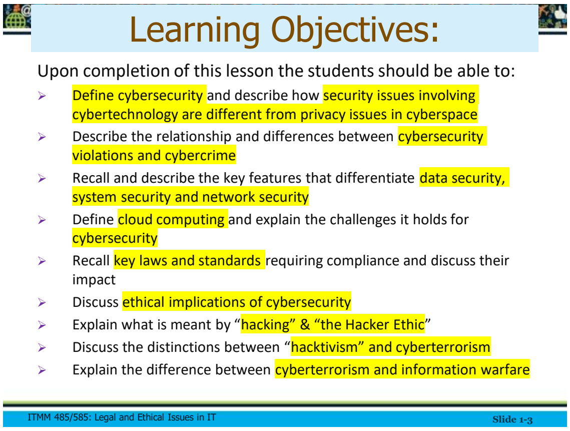
1

Ethical Concepts and Theories

ILLINOIS TECH | College of Computing

Ch6: Security and Compliance P4: Cloud Computing Security and Risk Management

2



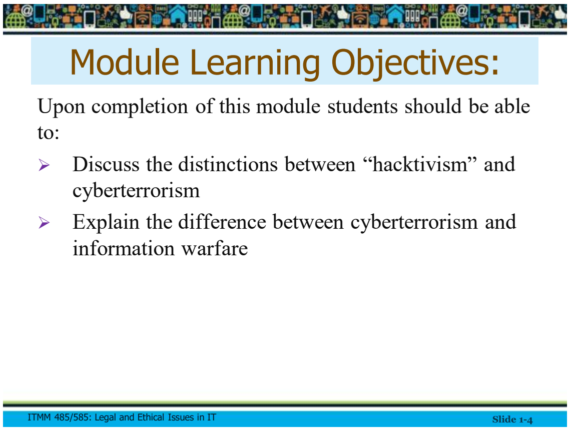
Learning Objectives:

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

- Define cybersecurity and describe how security issues involving cybertechnology are different from privacy issues in cyberspace
- Describe the relationship and differences between cybersecurity violations and cybercrime
- Recall and describe the key features that differentiate data security, system security and network security
- Define cloud computing and explain the challenges it holds for cybersecurity
- Recall key laws and standards requiring compliance and discuss their impact
- Discuss ethical implications of cybersecurity
- Explain what is meant by "hacking" & "the Hacker Ethic"
- Discuss the distinctions between "hacktivism" and cyberterrorism
- Explain the difference between cyberterrorism and information warfare

ITMM 485/585: Legal and Ethical Issues in IT Slide 1-3

3



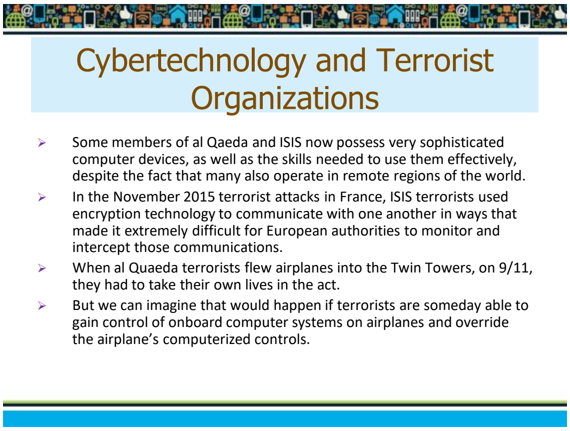
Module Learning Objectives:

Upon completion of this module students should be able to:

- Discuss the distinctions between "hacktivism" and cyberterrorism
- Explain the difference between cyberterrorism and information warfare

ITMM 485/585: Legal and Ethical Issues in IT Slide 1-4

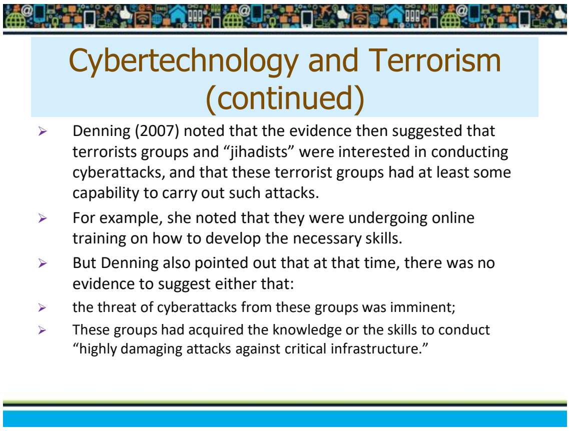
4



Cybertechnology and Terrorist Organizations

- Some members of al Qaeda and ISIS now possess very sophisticated computer devices, as well as the skills needed to use them effectively, despite the fact that many also operate in remote regions of the world.
- In the November 2015 terrorist attacks in France, ISIS terrorists used encryption technology to communicate with one another in ways that made it extremely difficult for European authorities to monitor and intercept those communications.
- When al Quaeda terrorists flew airplanes into the Twin Towers, on 9/11, they had to take their own lives in the act.
- But we can imagine that would happen if terrorists are someday able to gain control of onboard computer systems on airplanes and override the airplane's computerized controls.

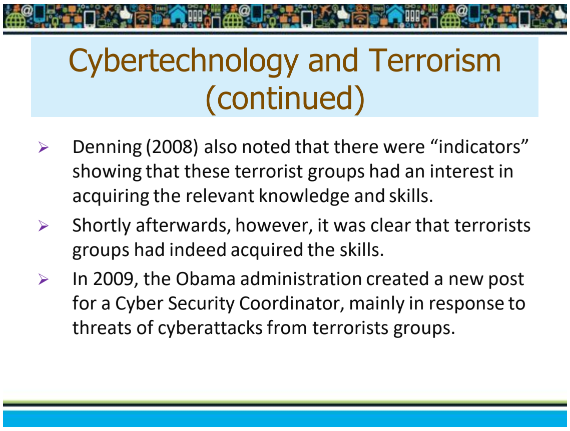
5



Cybertechnology and Terrorism (continued)

- Denning (2007) noted that the evidence then suggested that terrorists groups and "jihadists" were interested in conducting cyberattacks, and that these terrorist groups had at least some capability to carry out such attacks.
- For example, she noted that they were undergoing online training on how to develop the necessary skills.
- But Denning also pointed out that at that time, there was no evidence to suggest either that:
- the threat of cyberattacks from these groups was imminent;
- These groups had acquired the knowledge or the skills to conduct "highly damaging attacks against critical infrastructure."

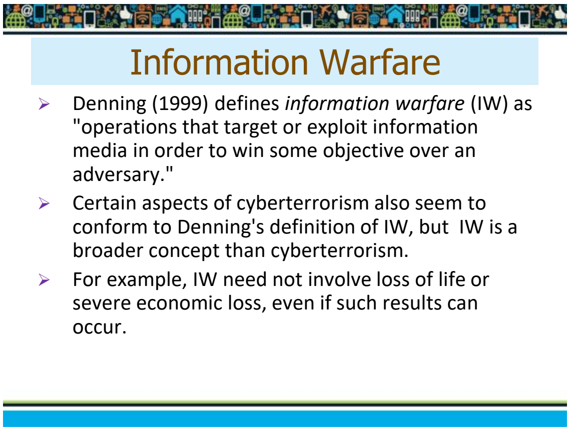
6



Cybertechnology and Terrorism (continued)

- Denning (2008) also noted that there were “indicators” showing that these terrorist groups had an interest in acquiring the relevant knowledge and skills.
- Shortly afterwards, however, it was clear that terrorists groups had indeed acquired the skills.
- In 2009, the Obama administration created a new post for a Cyber Security Coordinator, mainly in response to threats of cyberattacks from terrorists groups.

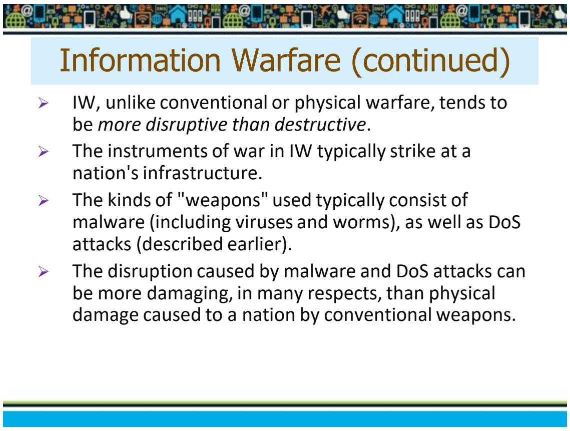
7



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.

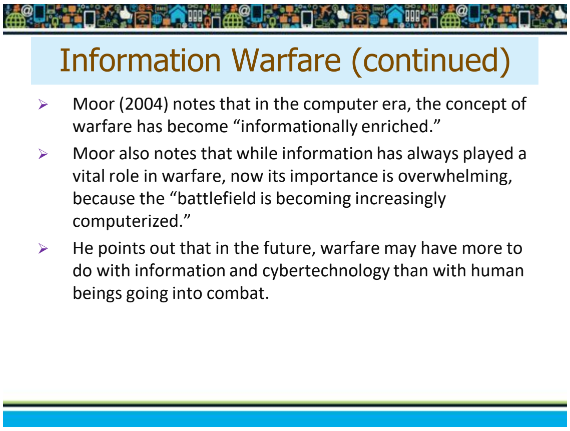
8



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 malware (including viruses and worms), as well as DoS attacks (described earlier).
- The disruption caused by malware and DoS attacks can be more damaging, in many respects, than physical damage caused to a nation by conventional weapons.

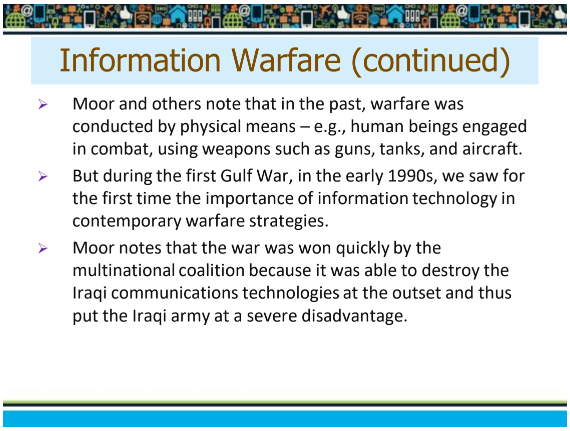
9



Information Warfare (continued)

- Moor (2004) notes that in the computer era, the concept of warfare has become “informationally enriched.”
- Moor also notes that while information has always played a vital role in warfare, now its importance is overwhelming, because the “battlefield is becoming increasingly computerized.”
- He points out that in the future, warfare may have more to do with information and cybertechnology than with human beings going into combat.

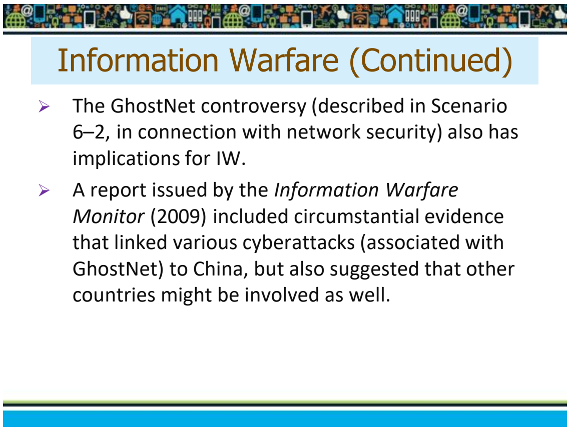
10



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.

11



Information Warfare (Continued)

- The GhostNet controversy (described in Scenario 6–2, in connection with network security) also has implications for IW.
- A report issued by the *Information Warfare Monitor* (2009) included circumstantial evidence that linked various cyberattacks (associated with GhostNet) to China, but also suggested that other countries might be involved as well.

12

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).

13

Information Warfare (continued)

- Review Scenario 6-1 (in the textbook) involving the Stuxnet Worm and the “Olympic Games” Operation.
- Does “Operation Olympic Games” qualify as an instance of IW (or “cyberwarfare”)?
- In so far as the Stuxnet worm sent misleading information to the Iranian government and its scientists, it complies with one aspect of IW.
- Also, because this worm was *disruptive* (regarding Iran’s nuclear program), as well as *destructive* (i.e., with respect to its effect on Iran’s centrifuges), it complies with another aspect of IW.

14

Information Warfare (continued)

- Additionally, consider that the Stuxnet attacks were launched (allegedly, at least) by two nation states.
- So, Stuxnet complies with all three elements of IW (described above).
- It is perhaps also worth noting that in the Olympic Games incident, there had been no formal declaration of war among the three nation states allegedly involved.

15

Information Warfare (continued)

- The Stuxnet worm, discovered in 2010, is sometimes confused with the Flame virus (also known as “Flamer” and “Skywiper”).
- The Flame virus also has implications for IW.
- Ladner (2012) points out that the Flame virus, discovered in 2012, is “an espionage tool” that can “eavesdrop on data traffic, take screenshots and record audio and keystrokes.”

16

Potential Consequences for Nations that Engage in IW

- In light of the Stuxnet attacks, some might ask if the U.S. and Israeli governments are now also guilty of the same kind of questionable behavior attributed to China and North Korea.
- Should the U.S. government worry about the possible repercussions that its involvement in “Olympic Games” could have for its standing in the international community, as well as for its credibility involving any future complaints that it might make against other nations, especially China?
- Sanger (2012) suggests that the United States did not think through the international implications of its use of cyberwarfare in the Olympic Games operations (just as he believes that it also did not think through some of the major political and legal consequences of its policy regarding use of armed drones).

17

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.

18

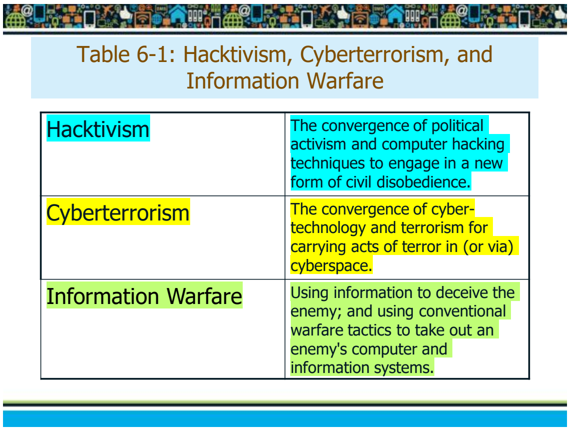


Table 6-1: Hacktivism, Cyberterrorism, and Information Warfare

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.

19

?

ITMM 485/585: Legal and Ethical Issues in IT

Slide 1-20

20