Computers as a Tool of Terrorism

- SRA-211, Threat of Terrorism and Crime
- Penn State Altoona
- Larry Garvin

Technology and War

- Warfare has evolved parallel to the development of tools and technology
- Traditional warfare has been altered by technology. For example, the use of civil aircraft as a weapon
- Attacking a nation's critical infrastructure is another such evolution of warfare
- Protecting our critical infrastructure is a large part of our national plan for homeland, but is ignored by the public

Information Warfare/Cyberterrorism

- Not the same
- Cyberterrorism is a subset of information warfare
- Information warfare is not necessarily cyberterrorism
- If your network is disrupted by Chinese government hackers and has to be taken offline for repairs, this isn't really cyberterrorism. You aren't terrorized by the attack, but it is information warfare

Information Warfare

- Gathering or using information to gain an advantage over another entity
- Information warfare is not limited to computers
- Any disruption to an information system would be considered information warfare
- Includes everything from hacking into a computer system to knocking down a cell phone tower with a bulldozer

Information Warfare 6 Components

- Psychological operations: Using information to affect an adversary's state of mind
- Electronic warfare: Denial of information or accurate information to an adversary
- Military deception: Mislead an adversary about military capabilities or intent
- continued …

Information Warfare 6 Components

- Physical destruction: Direct attack on an information system to destroy it
- Security measures: Methods of protecting an information system so that it cannot be breached
- Information attack: Corruption of information without changing the physical structure of its location

Defining Cyberterrorism

- It is sometimes difficult to determine when a cyberterrorist attack actually constitutes terrorism
- Cyberterrorism is also not defined by who is carrying it out. It is defined by what it is
- Cyberterrorism is a premeditated, politically motivated attack against information, computer systems, programs or data that results in violence to civilian targets. "Hacking with a body count."

4 Categories of Attack

- Infrastructure attack: Attacks designed to destroy a system that includes critical data
- Information attack: Attacks focused on destroying or altering electronic files or computer systems
- Technological facilitation: Using cyber communications to plan a terrorist attack, incite an attack, or otherwise support terrorism
- Promotion: Fundraising, solicitation and recruitment

US at High Risk for Cyberattack

- Political issues in the Middle East
- Radical Islam opposes modernity as a threat to Islam
- Anti American sentiment in the Muslim world
- Anti capitalist movements in China and North Korea with possibly state supported attacks
- Reliance on a national information infrastructure makes the US extremely vulnerable

Info Infrastructure Components

- Communication networks such as phones and satellites
- Provision of information such as TVs and radios
- Information resources such as educational or medical programs and resources
- Applications used for electronic commerce
- People

Clinton Critical Infrastructure

- Telecommunications
- Banking and finance
- Electrical power relies on electronic sensors
- Oil and gas distribution and storage
- Water supplies rely on electronic sensors
- Transportation such as aviation systems
- Emergency services
- Government services

Demonstrated Infrastructure Attacks

- In 1997 a teenager hacked into the phone system at Worcester Airport in MA. The subsequent disruption in phone service caused delayed and canceled flights across the country resulting in substantial financial losses
- A former Chevron employee disabled an alert system for a plant by hacking into company computers. Chevron was unaware when the system released noxious chemicals into the air because the sensors were turned off

Risk is Unknown

- Difficult to quantify just how at risk our infrastructure may be
- There has never been a complete analysis of weaknesses in our infrastructure

Information Attacks

- Focused on destroying or altering content
- Tend to be more disruptive than destructive
- Web site defacements are one trivial example
- Viruses and worms
- Distributed denial of service attacks
- Unauthorized intrusions

Facilitation

- Using computers to support the attack including communications, recruitment and propaganda
- Faster, lower cost communication between terrorists
- Allows more effective decentralization which keeps them safer because they can communicate more effectively

Data Hiding

- Secrets can be hidden pictures, sound files or word processing files. Software is available that allows messages to be easily hidden inside of a picture file
- It is believed that al Queda has hidden maps and instructions to other terrorists in plain view in things like pornographic files that anyone can download

Cryptography

- Cryptography is used to secure communications between terrorists
- al Queda couriers have been captured with encrypted files

Propaganda and Promotion

- The Internet is a particularly effective tool for those looking to spread messages of hate and to recruit new members
- Most terror groups have a website

Cyberterrorism as Adjunct Attack

- Cyberterror attacks are likely to be most effective when they are combined with other types of attacks
- This will compound and enhance the effect of the original attack. In military terms, this is referred to as a force multiplier

al-Queda and Information Technology

- It is believed that al Queda makes sophisticated use of the Internet
- In 2002 al Queda was actively working on a cyber jihad directed at the stock market

Attacks on Grids

- In 2001, the FBI discovered a series of network intrusions into telephone, electrical, water, nuclear and gas systems, all of which had been routed through telecommunication systems in Saudi Arabia, Pakistan and Indonesia
- In 2002, an al Queda computer seized in Afghanistan contained information from these probes
- Seized al Queda computers have contained information on the digital switches used to run transportation and power grids

China and Information Warfare

- China has a program in information warfare
- They have assembled teams of hackers trained to engage the United States in cyber warfare and has already likely used these teams
- Multiple intrusions into American systems have been traced back to China
- No proof has even been discovered of Chinese government involvement, but given this history of how things work in China, these attacks were likely ordered by the government