Cyberterror

Cyberspace – computer-mediated communication systems – has become a battleground between states and terrorists, and among nation states.

Cyberterror – use of computers and telecomm technologies to attack & severely disrupt physical infrastructures; or to make electronic threats; or to exchange information among terrorists

Cyberwar – tactical or strategic use of cyberspace to gain military advantages over an enemy

What are terrorists' main uses of cyberspace?

How does cyberterror resemble and differ from hack attacks and criminal misuse of the Internet?

How vulnerable are U.S. defense systems and national infrastructure to cyberterrorism?

What nations cyber spy on U.S.? What is Stuxnet?

What policies have the U.S. adopted to defend cyberspace & how might they impact our rights?

Terrorists on the Internet

Almost all major foreign terrorist organizations have Websites and use the Internet to communicate, coordinate, propagandize, recruit participants.

- Fundraising by donor appeals, selling goods
- Training manuals & weapon-making instruction
- Martyrdom videos & films of attacks, beheadings
- Chatrooms, emails using coded language, symbols
- Threats, disinformation, hoaxes to divert attention

Anwar al-Awlaki, an American of Yemeni descent, is a cleric who used the Internet to mentor and motivate the Fort Hood shooter and Times Square bomber from hideout in Yemen. His sermons were attended by three 9/11hijackers. Alleged Al-Qaida regional commander, he may have trained the underwear bomber in 2009.

Awlaki posts blogs, Facebook page, YouTube videos

Pres. Obama approved him for “targeted killing” by CIA, first ever of a U.S. citizen. So far unsuccessful …

http://www.youtube.com/watch?v=gQRrYCUeFt0

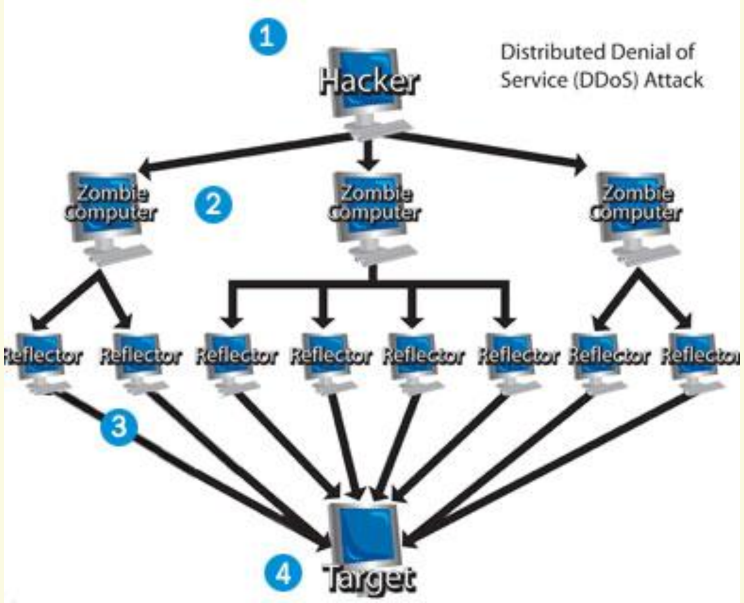
Hack Attacks

Beyond exchanging information, terrorists might use cyberspace to attack government & private infrastructures to disrupt, disable, & damage systems.

“Hackers” – cybercriminals – have grown increasingly skilled at malicious computer security breaches, unleashing viruses, worms, trojans, …

A distributed denial of service attack floods a targeted computer system with so many external requests that it cannot respond effectively to legitimate users.

A hacker gains remote control of several “zombie” agents, which send packets to “reflector” machines that seem to be requests for information coming from the target. Reflectors bombard the target until it slows or shuts down completely.



A trojan horse program may be unwittingly inserted into a computer, which then downloads undetected program that takes over key functions of the computer and communicates secretly with the hacker.

Using this hidden connection, hackers can compromise software and plunder files. Terrorists could gain control over of critical infrastructure.

http://computer.howstuffworks.com/zombie-computer3.htm

Cyber War!

Watch Frontline's *Cyber War!,* in which experts discuss how terrorists could use the Internet to launch major attacks on national infrastructure.

> **"The critical infrastructure of the U.S., including electrical power, finance, telecommunications, health care, transportation, water, defense and the Internet, is highly vulnerable to cyber attack. Fast and resolute mitigating action is needed to avoid national disaster."**
>
> **Open letter from 54 scientists to Pres. Bush (2002)**

What did the Pentagon's "Eligible Receiver" exercise reveal about the potential for hackers to take control of our national defense systems?

How vulnerable is the U.S. to cyber attacks, compared to physical terrorist assaults? What are Al-Qaida's cyberterror capabilities?

Why are digital Supervisory Control and Data Acquisition (SCADA) systems – which manage our vital infrastructures – America's weak link?

Has the federal government been too lax about cyber security strategy? What should and can be done to strengthen U.S. cyber security?

Cyber War vs. Cyber Espionage

Cyber attacks often launched by geeks seeking fun & criminals seeking profits. Terrorists have launched few politically motivated cyber attacks.

2007 Russian cyber attack on Estonia Websites after relocation of a Soviet war memorial*

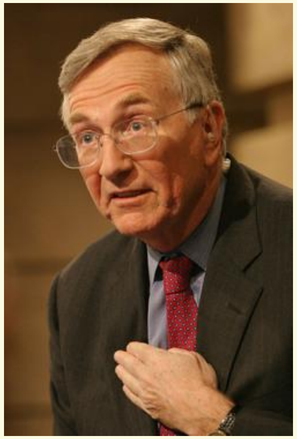
2008 Russian hackers attack Georgia's Internet before Russia's invasion to secure enclaves

2008 Chinese Internet addresses email viruses to organizations supporting Tibetan protests

2009 Russian "cyber-militia" DDoS shuts down Kyrgystan's Internet service

* http://www.youtube.com/watch?v=9JnXrtLIp1k&NR=1

States are primary instigators or threats to use cyber attacks against other nations. United States was slow to recognize & to improve cyber security.



Richard Clarke & Mike McConnell built cyber-consulting firms, but Seymour Hersh remains skeptical about the real scope of danger:

"I was told by military, technical, and intelligence experts that these fears have been exaggerated, and are based on a fundamental confusion between cyber espionage and cyber war. … Blurring the distinction … has been profitable for defense contractors – and dispiriting for privacy advocates."

China & Russia Spy on U.S.

In 2008, Director of National Intelligence Mike McConnell reported 3 million daily unauthorized probes of Defense Department computer networks. State Department fought off two million probes daily. Pentagon spent $100M in six months to April, 2009, to respond to and repair damage from cyber attacks.

HE'S GONE: Jerry Garcia Dead at 53
TIME
CYBER WAR
The U.S. rushes to turn computers into tomorrow's weapons of destruction. But how vulnerable is the home front?

June 2007: Suspected People's Liberation Army hackers caused a partial shutdown of a computer system serving Defense Secretary Gates' office.

March, 2009: Cyber spy network of servers mainly based in China tapped into classified documents from government & private orgs in 103 countries, including the computers of Tibetan exiles.

April 8, 2009: National security officials said, "Cyberspies [from China, Russia, other countries] have penetrated the U.S. electrical grid and left behind software programs that could be used to disrupt the system...

"Authorities investigating the intrusions have found software tools left behind that could be used to destroy infrastructure components, the senior intelligence official said. He added, 'If we go to war with them, they will try to turn them on.'"

http://online.wsj.com/article/SB123914805204099085.html

Stuxnet

Stuxnet computer worm crawled into Web in June 2010. It spies on and reprograms industrial systems, especially critical infrastructure (SCADA).

60% of infected computers were in Iran, targeting Siemens systems. In November Iran confirmed Stuxnet had damaged nuclear program at Natanz & delayed Bushehr Nuclear Power Plant start up.

By making rapid changes in centrifuge rotation speeds, it can cause these uranium-enrichment machines to spin out of control and fly apart.

China and India infected even worse than Iran, but damage wasn’t severe. Rupert Murdoch’s Sky News reported that Stuxnet, or variant virus, was possibly “traded to a criminal gang or terrorist group.”

Because of its complex computer code and the specific system Stuxnet targets (e.g., variable-frequency drives from two vendors used by Iran), others saw Israel as the most likely source, to delay Iran’s nuclear program.

Head of Iran’s Info Tech Co.: “The attack is still ongoing and new versions of this virus are spreading.” Iran’s top Stuxnet expert was killed in a bombing on November 29, the fifth such attack on nuclear personnel in past two years.

How to Increase Cybersecurity?

Cybersecurity responsibility is split between military & civilian Homeland Security Dept. Sy Hersh reported bureaucratic fights over budget and turf.

Deputy Defense Sec. Lynn wrote: “As a doctrinal matter, the Pentagon has formally recognized cyberspace as a new domain of warfare.”

Hersh: “This definition raises questions about where the battlefield begins and where it ends. If the military is operating in ‘cyberspace,’ does that include civilian computers in American homes?

Is federal regulation of private cybersecurity – setting and enforcing mandatory standards & certifying professionals – necessary?

Should “Cyber Czar” or the President have the power to shutdown government, military, & civilian networks if a cyber attack occurs?

How far can we trust the federal government not to abuse its authority to protect U.S. communications & infrastructure networks?

What steps should be taken to improve cyber-intelligence gathering, while still preserving all of our civil liberties and rights?