

Cyber Terrorism



b6
b7C
b7E

Supervisory Special Agent
FBI San Francisco

13 March 2004



Terrorist Groups



Terrorist Use of the Internet

- Facilitation
 - "The three C's"
 - Command
 - Control
 - Communications
- Attacks
 - Hacktivism
 - Conventional Cyberterrorism:



Terrorist Exploitation of the Internet Command/Control/Communications



Terrorist Use Of Cyber Technology – Non Attack

> Command/Control/Communication

b7E

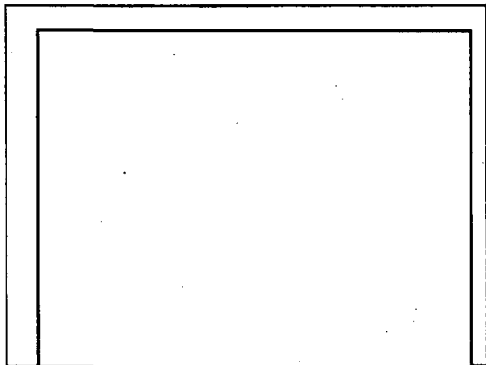


> Advertising

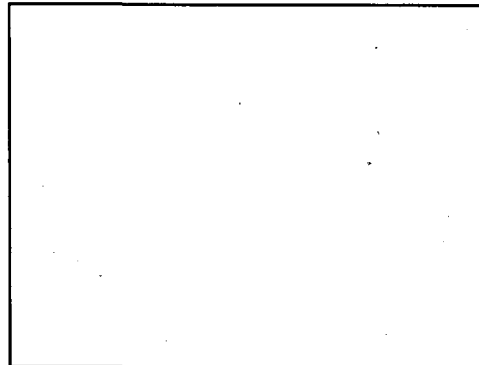


b7E

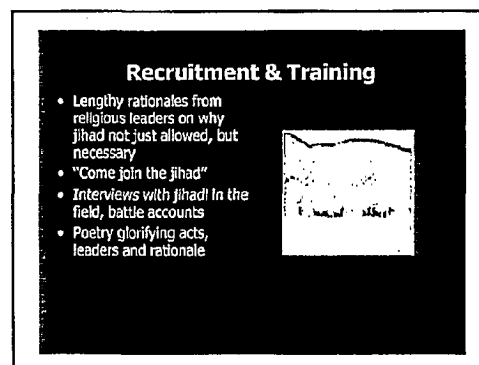
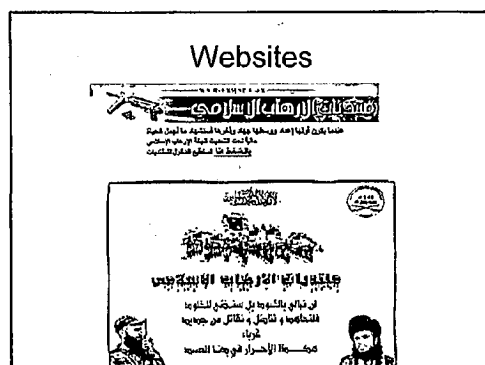
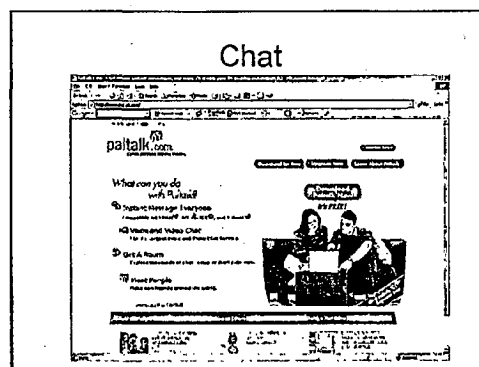
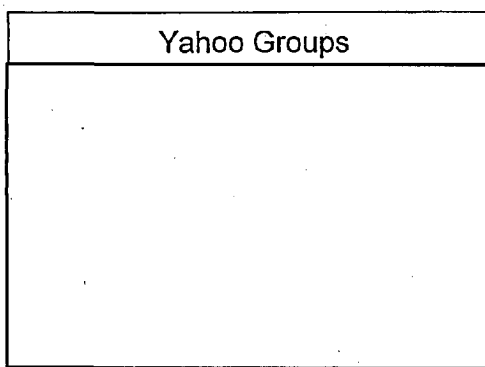
b7E

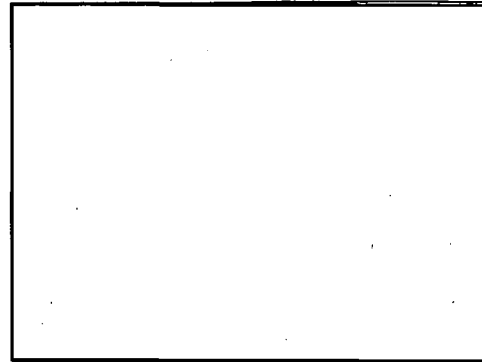
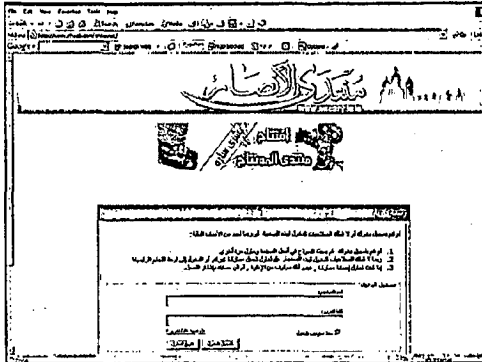


b7E

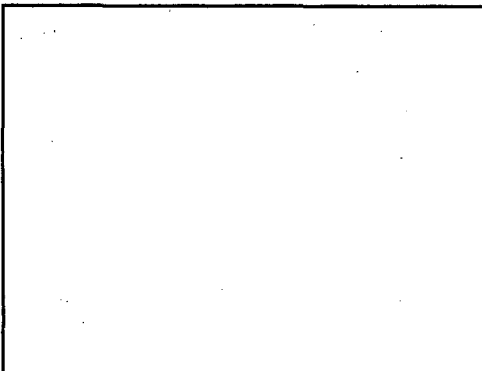


b7E

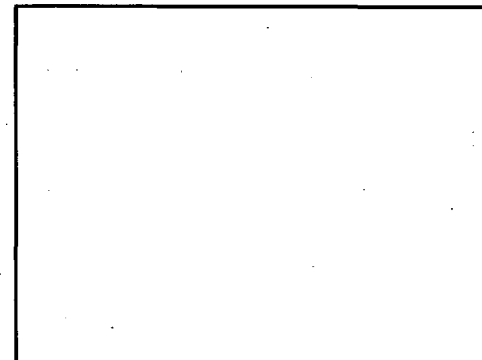
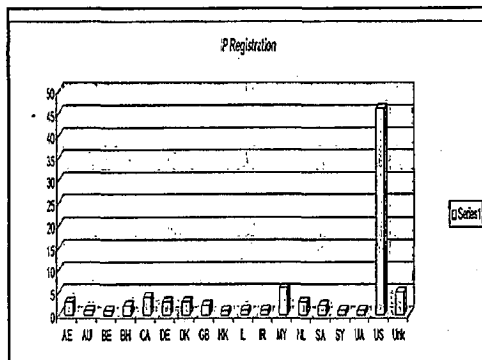
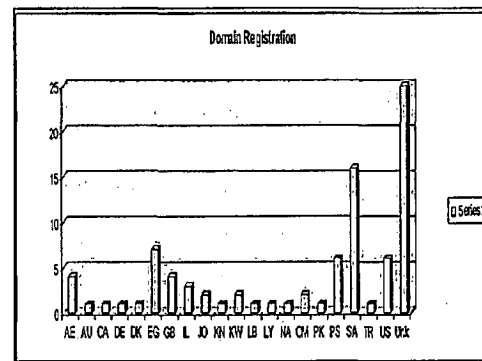




b7E

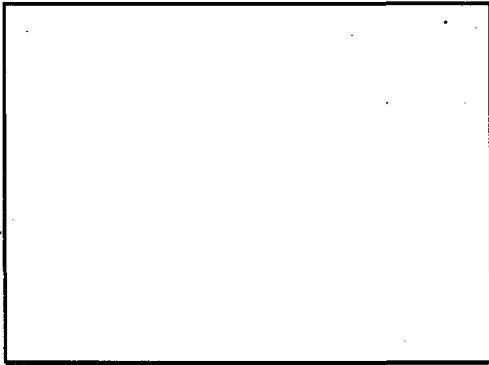


b7E

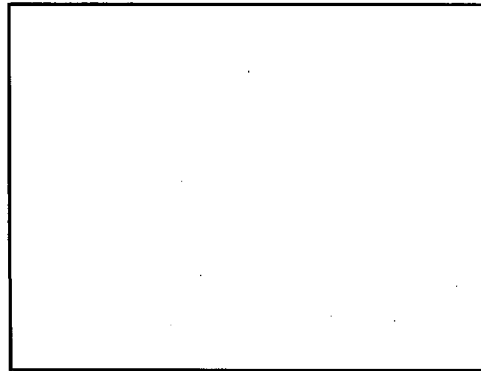


b7E

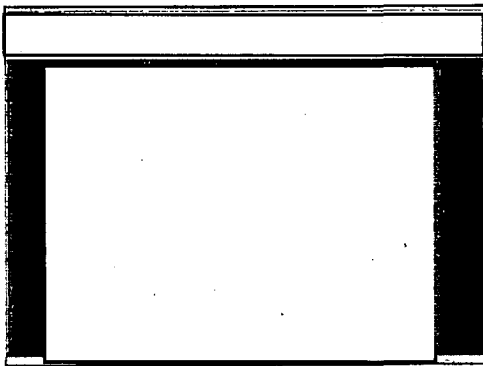
b7E



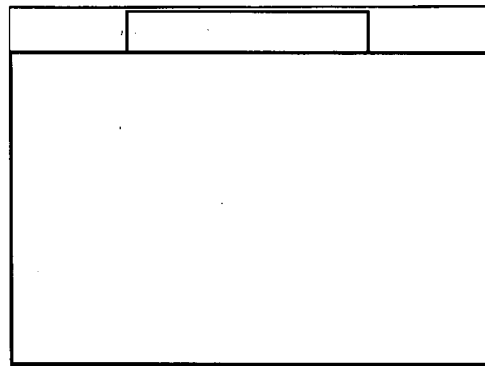
b7E



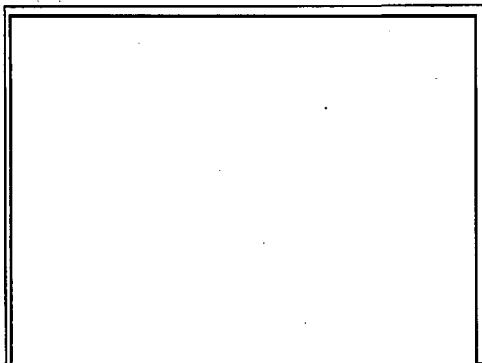
b7E



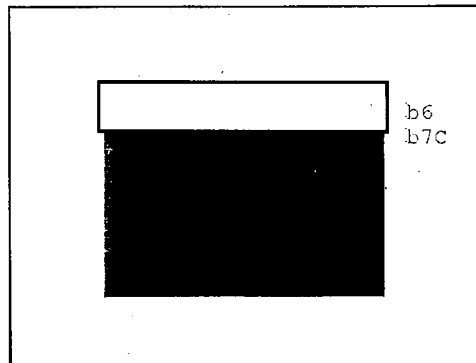
b7E

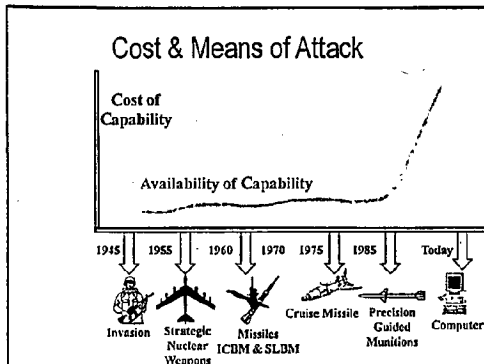


b7E



b6
b7C





Cyberterrorism

- Types of Attacks
 - Website defacement**
 - More of a nuisance than threat
 - Denial of service**
 - Easiest to do
 - Can cause severe disruptions, but only temporarily
 - Intrusion**
 - Provides access to data

b7E

Cyberterrorism

- Types of Activities
 - E-mail cracking**
 - Used to vet recruits
 - Used to gather intell on enemies
 - E-jihad tutorials**
 - Manuals (fairly basic)
 - Classes
 - Offerings of e-attack software and Vulnerabilities**
 - Software piracy and Internet financial fraud**

Techniques / Examples

Hactivism

Denial of Service (DoS)

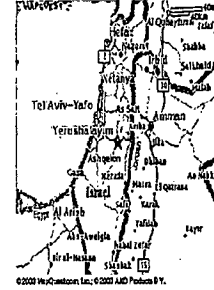
- Flood a server with network traffic (usually malformed data packets), denying valid users access to the services of the computer.
- Attack Methods: ICMP, UDP, SYN Floods, and Smurf.

Distributed Denial of Service

- DDoS –Denial of Service on steroids. An attacker (Bot Herder) controls an army of slave computers, called "agents" or "bots", to perform a coordinated denial of service attack.
- Attack tools are freely available on the Internet: Trinoo, TFN, Stacheldraht, and TFN2K are examples.

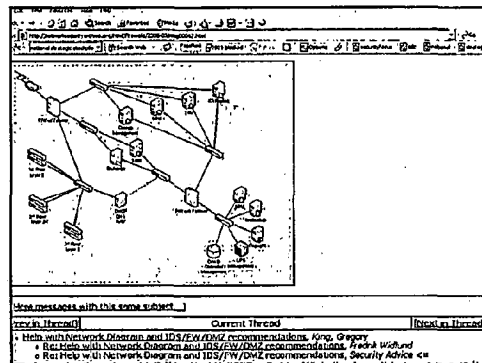
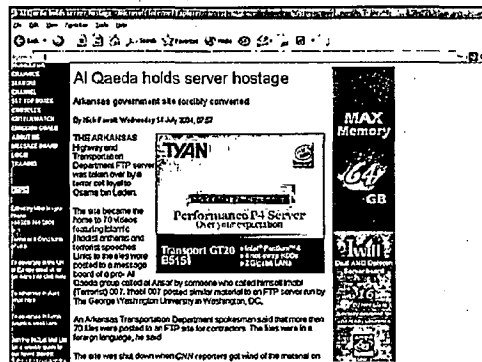
Palestinian-Israeli Cyber Wars

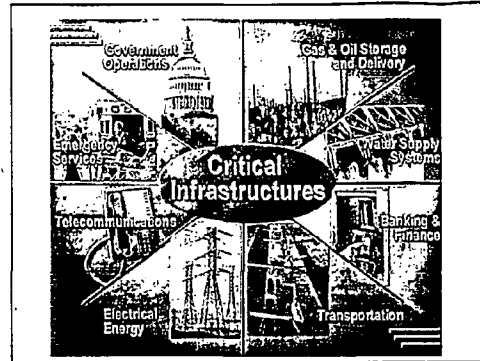
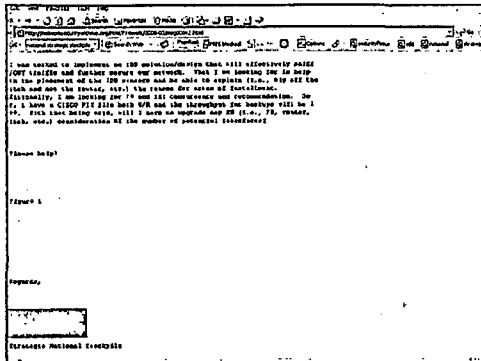
- September 2000
- Israeli hackers (reportedly teens) DoS attacked Hezbollah and Hamas sites in Lebanon
- Wizel.com
- FloodNet attack
- Pro-Palestinian hackers attacked Wizel and Israeli e-business sites
- Horizontal Escalation
- Spilled over borders
- Continued through approx April 2002



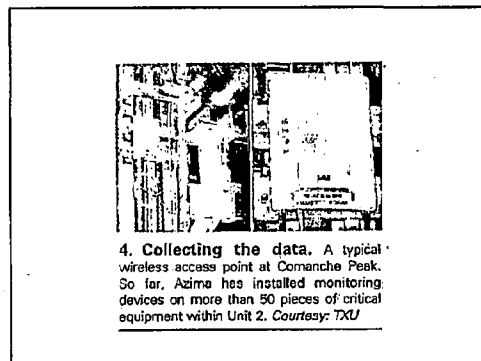
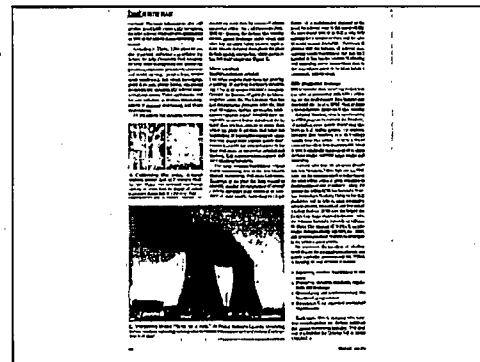
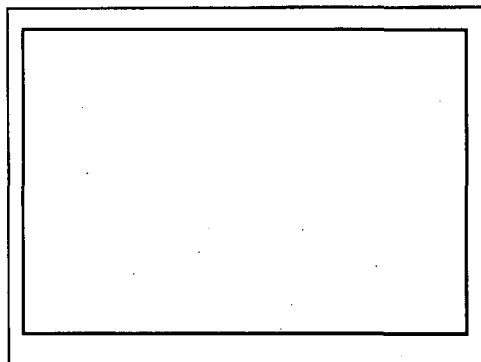
Computer Intrusions

- Intruders gain access by various methods such as using exploits for a particular computer system or exploiting a weak account password. (Goal is to gain root or administrator privileges)
- Results
 - Theft and/or destruction of sensitive data
 - Computer network damage
 - Control of computer for other uses (BOT networks, DDoS attack)
 - Set up a Jihadi FTP Site

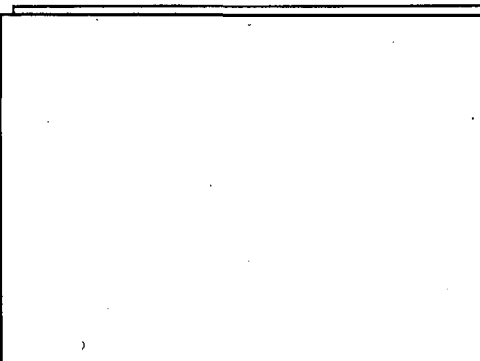


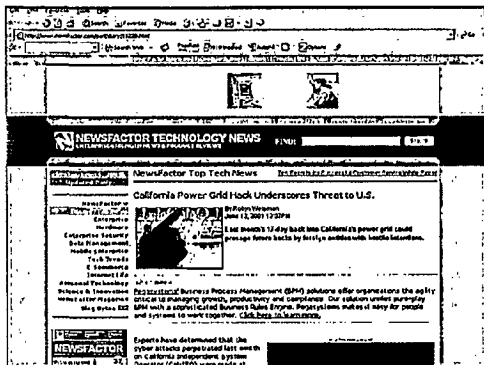


b7E



b7E



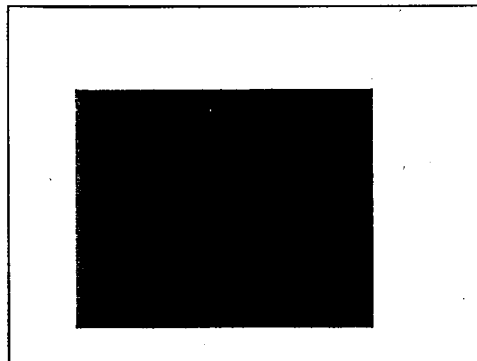
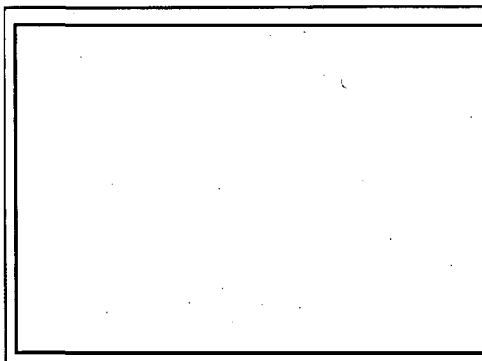


Worm infects Nuclear Power Plant

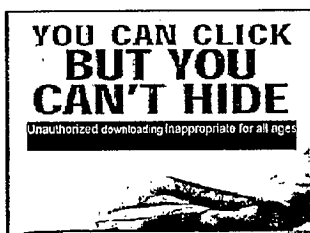
- ❑ Ohio's Davis-Besse Nuclear Power Plant
- ❑ January 2003
- ❑ Slammer worm
- ❑ Disabled safety monitoring system for five hours but there was a redundant system
- ❑ Entered through contractor network



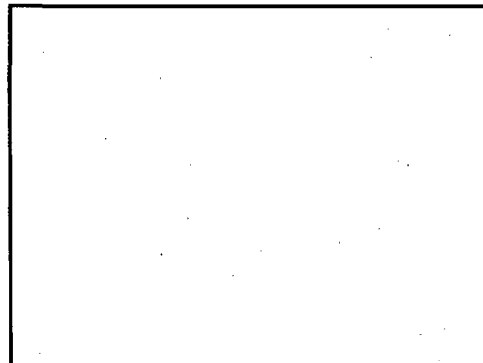
b7E



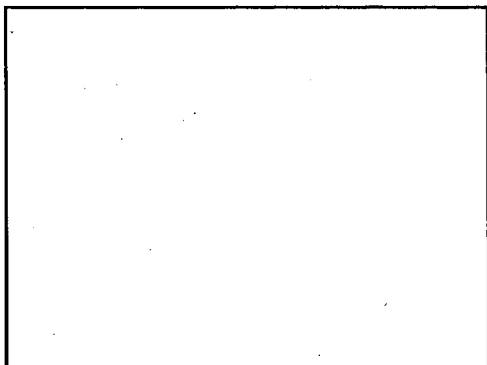
▪ Cyber Counter Espionage



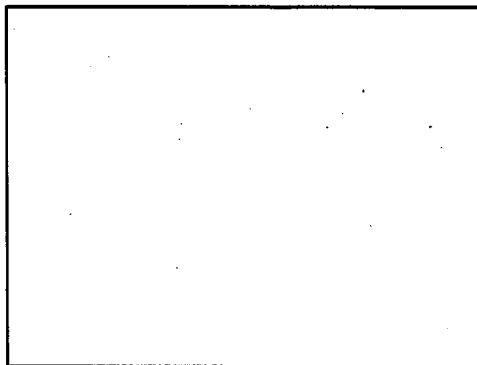
b7E



b7E



b7E



QUESTIONS ??



Contact

SSA [redacted] FBI San Francisco

b6
b7C

151fench 2004