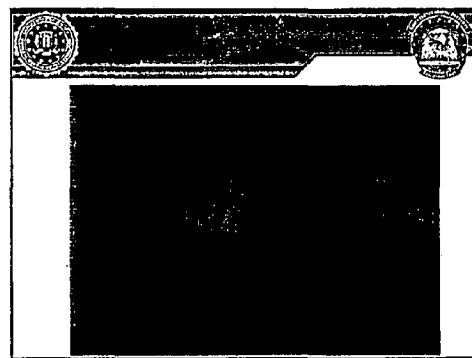
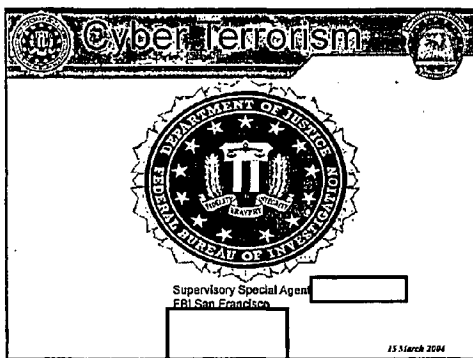
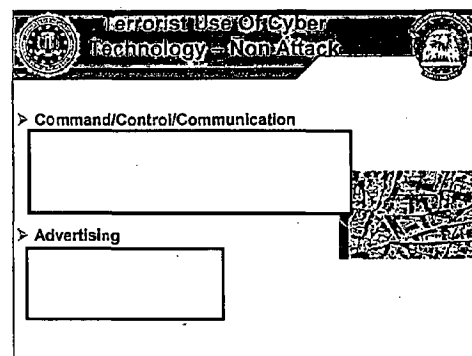
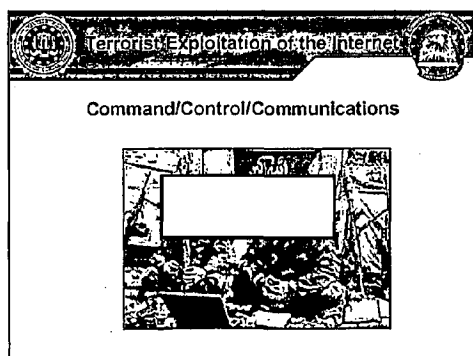
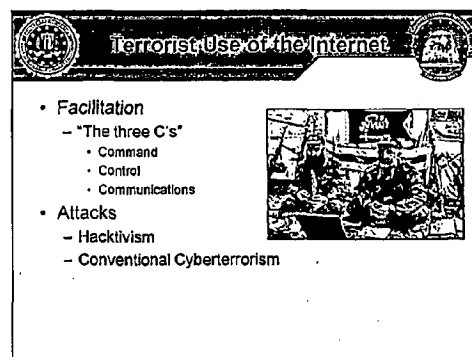
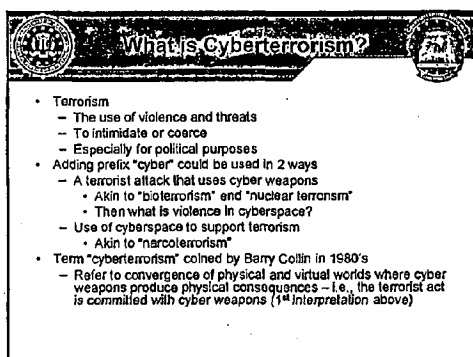
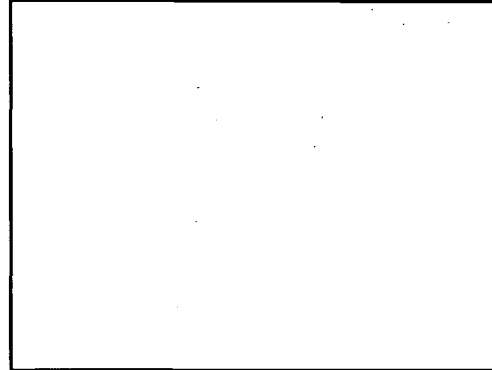
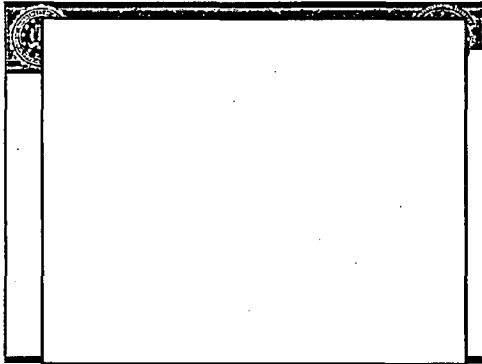




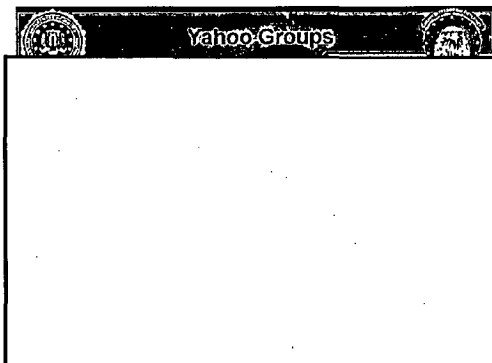
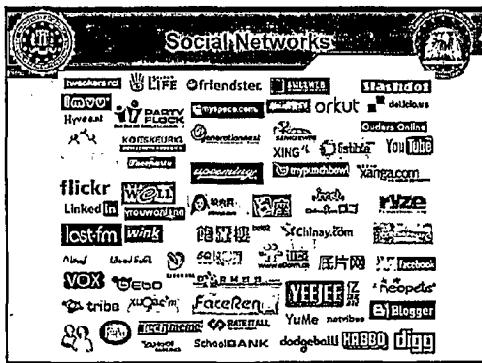
b6
b7C
b7E



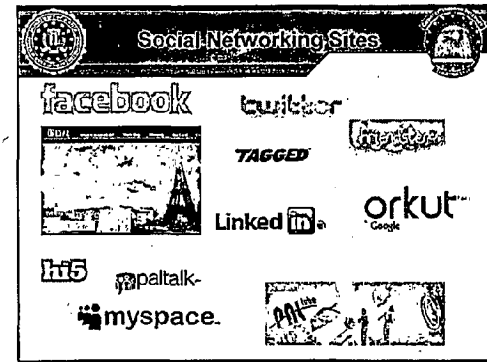
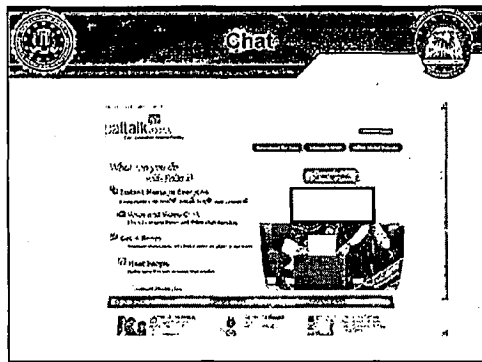
b7E



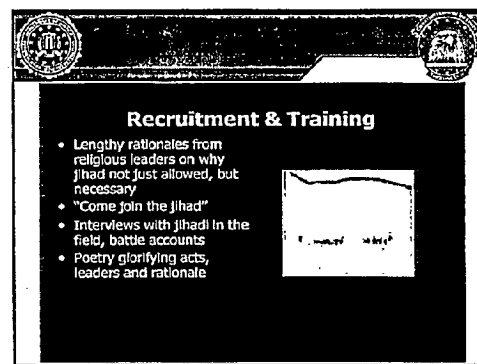
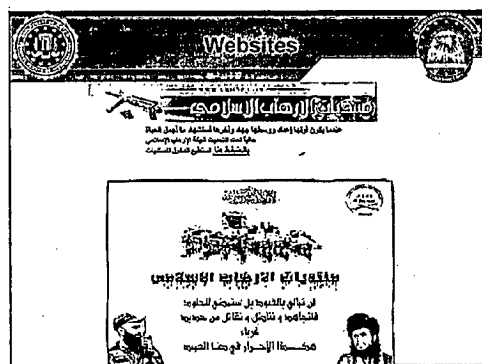
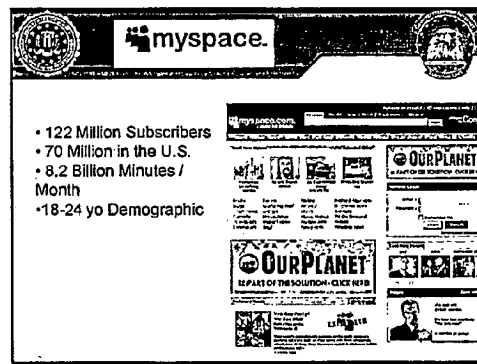
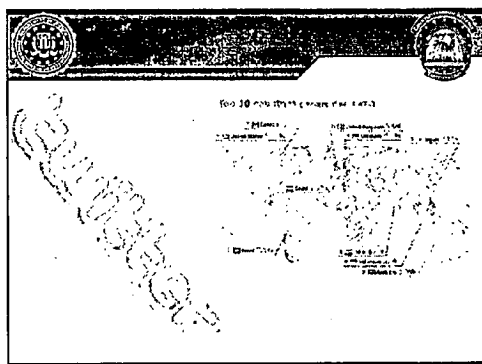
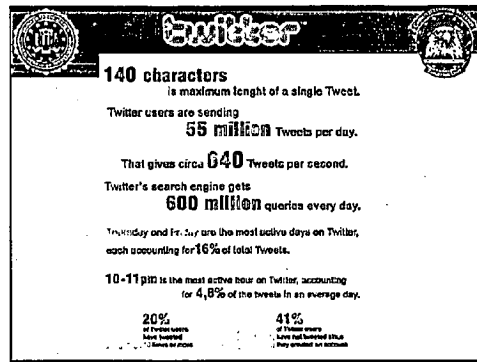
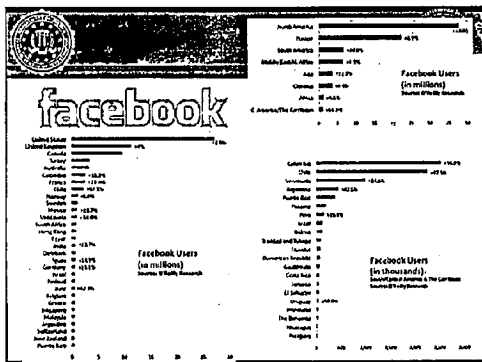
b7E

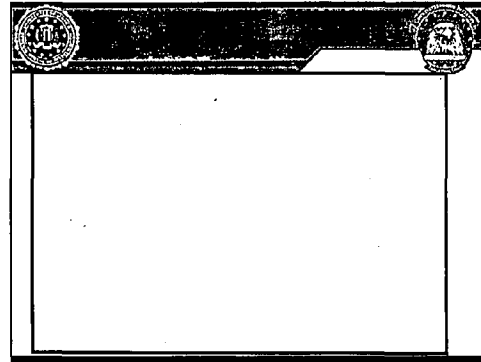
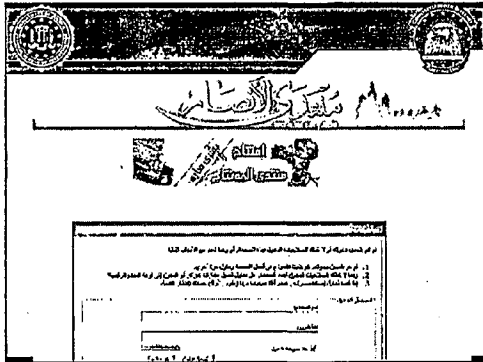


b7E

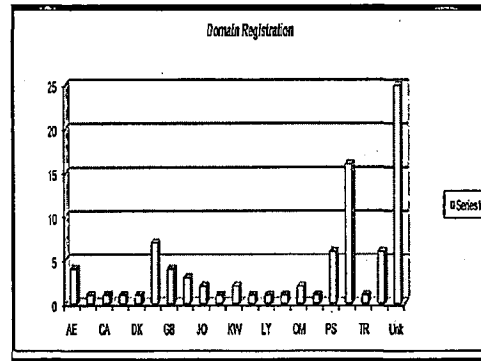
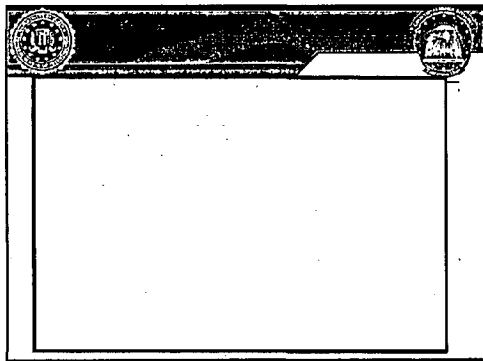


b6
b7C

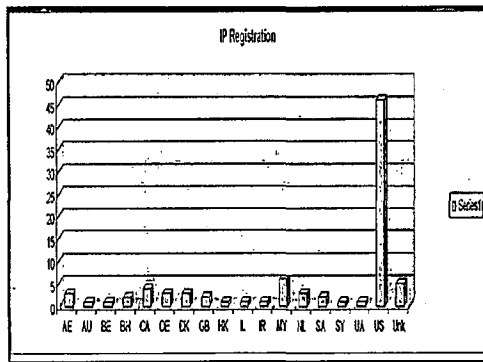




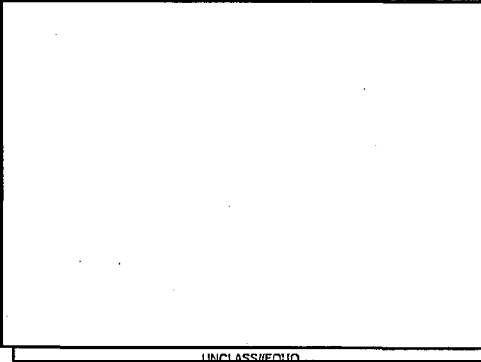
b7E

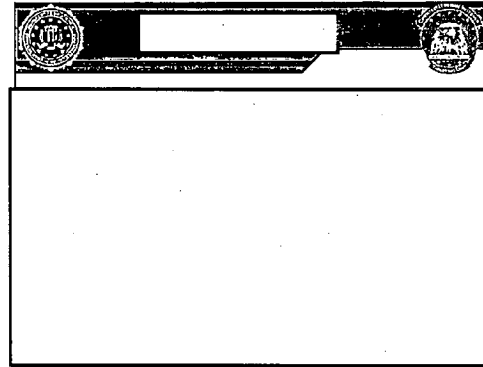
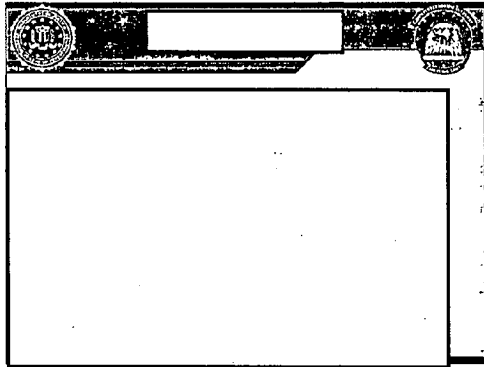


b7E

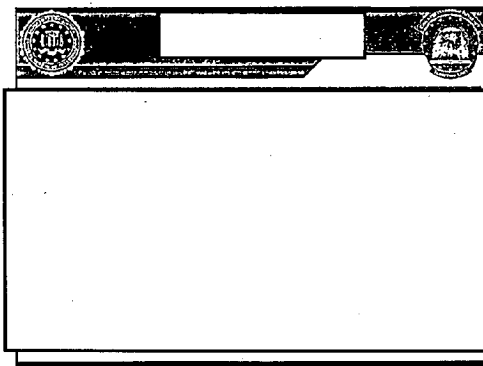
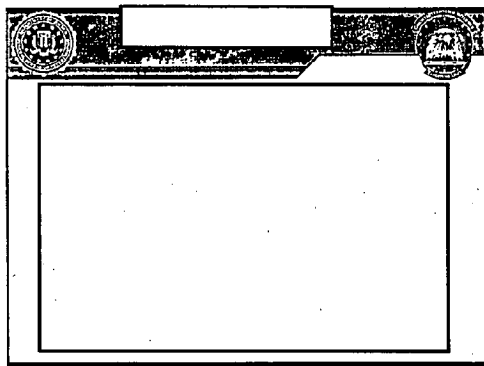


b7E

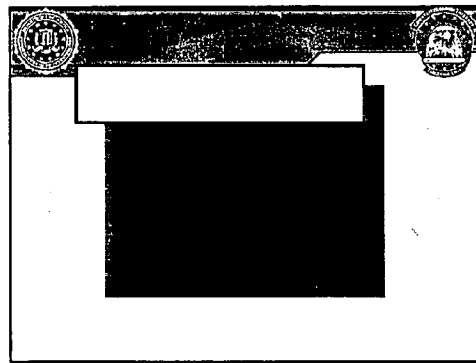
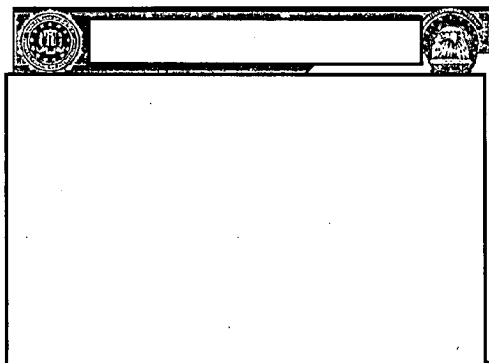




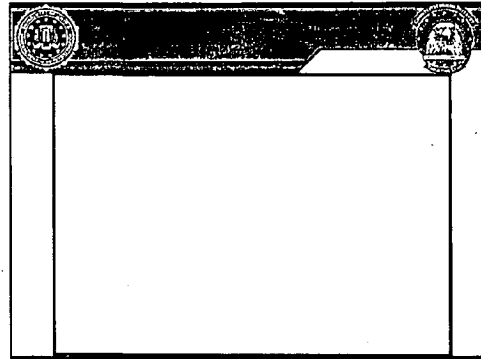
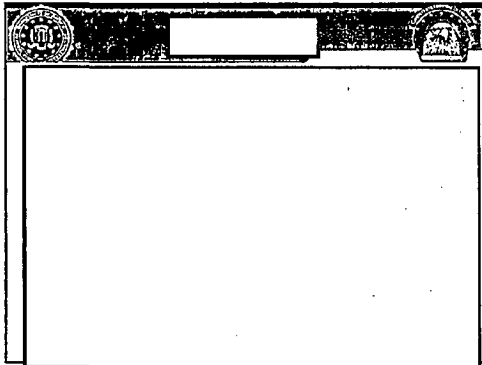
b7E



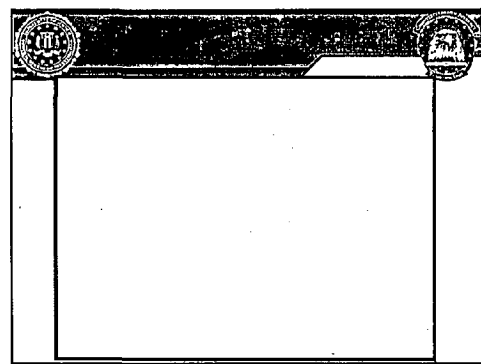
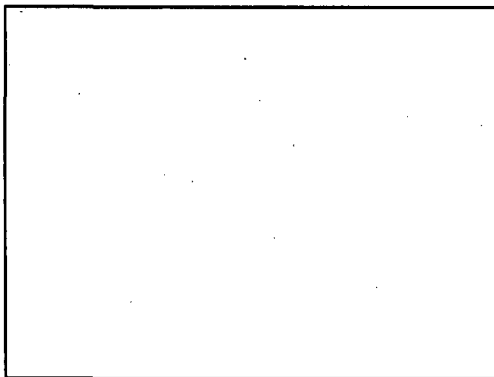
b7E



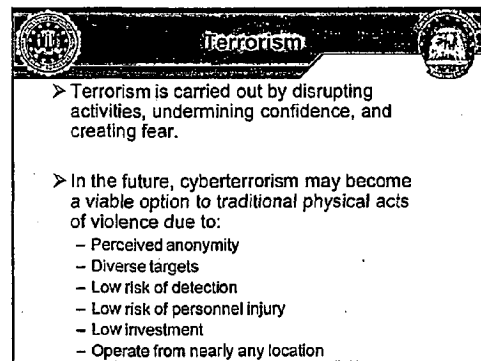
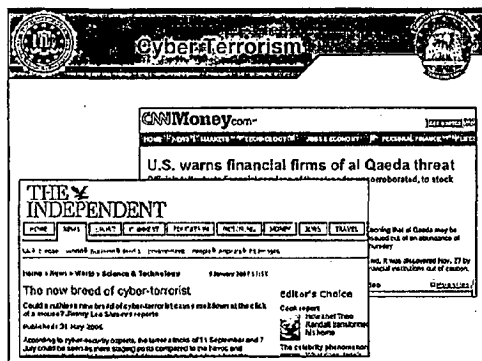
b7E

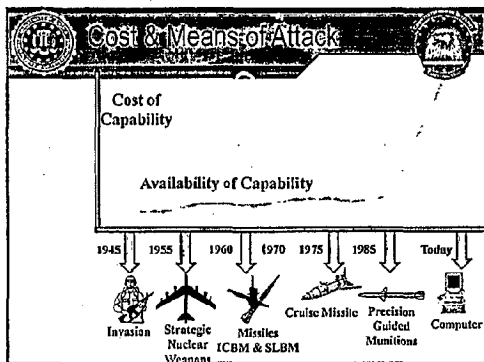


b7E



b7E





"Hacking, Why Not?"



- By Imam Samudra
 - Sentenced to death for 2002 Bali bombings
- Book chapter in *Me Against the Terrorists*, 2004
 - Written in prison
- Advocates cyber attacks to raise money, especially via credit card fraud, and "bring America and its cronies to its knees."
- Fundimentary guide to hacking (mainly "carding") methods and resources
- Credit card numbers found on his computer

Statements About Cyber Attacks

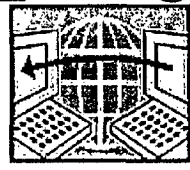
- After 9/11, OBL allegedly told Haidid Mir (ed, Ausaf newspaper)
 - "... hundreds of Muslim scientists were with him and who would use their knowledge in chemistry, biology and (sic) ranging from computers to electronics against the infidels."
- Dec 2001
 - suspected member of al Qaeda, said in
 - Terrorists had penetrated Microsoft and attempted to plant Trojan horses and bugs in Windows XP. [Newsbytes]
- Sheikh Omar Bakri Muhammad, London-based head of al-Muhammadiyah, told *Computer World* in Nov 2002
 - "... would not be surprised if tomorrow I hear of a big economic collapse because of somebody attacking the main technical systems in big companies."
- Principle 34 (electronic jihad) of *The 39 Principles of Jihad*, 2003
 - Directs computer users to use their skills and experience in destroying American, Jewish and secular websites

Statements About Cyber Attacks

- Fouad Hussein, *al-Zarqawi-al-Qaeda's Second Generation*, 2005, in Arabic
 - Describes 7 phases of al-Qaeda's long-term war based on interviews of top lieutenants
 - Phase 4, 2010-2013, includes cyberterrorism against US economy
- jihadi al-Farooq web forum, www.al-farooq.com/ab - 2005
 - Postings call for cyber attacks against US and allied government websites
 - Participant "achraf" proposed forming an operations unit within the Islamic Hacker Army (Jaiish al-Hacker al-Islami)
- Al-Ekhlaas web forum posting on Sep 11, 2006
 - Proposals to counter "Crusader media campaign in Iraq"
 - One proposal is for a group of young hackers to disable websites that attack Islam, jihad, etc, including www.ngterror.info
- Statements about inflicting economic damage
 - Numerous postings about using cyber attacks to achieve this

b6
b7c

What do They Do?


ZARQAWI'S IN CYBERSPACE

GUIDE TO ANALYSIS & RESPONSE

Cyberterrorism

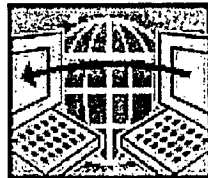
- Types of Attacks
 - Website defacement
 - More of a nuisance than threat
 - Denial of service
 - Easiest to do
 - Can cause severe disruptions, but only temporarily
 - Intrusion
 - Provides access to data

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



Hacktivism



Denial of Service (DoS)

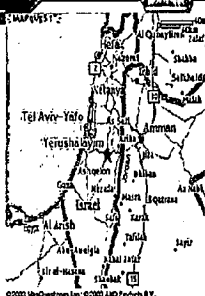
- Flood a server with network traffic (usually malformed data packets), denying valid users access to the services of the computer.
- Attack Methods: ICMP, UDP, SYN Floods, and Smurf.

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) DDoS 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

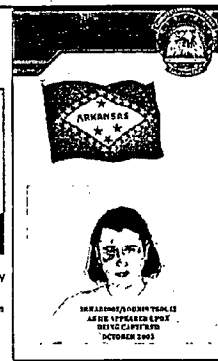


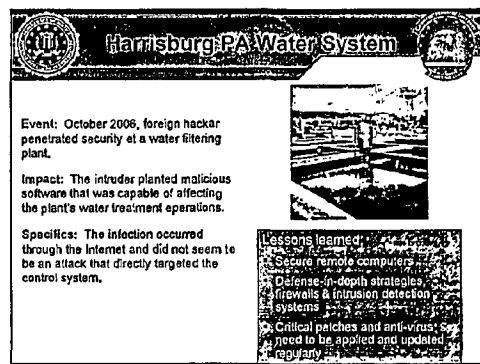
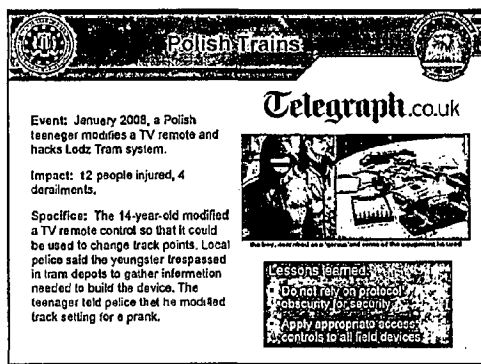
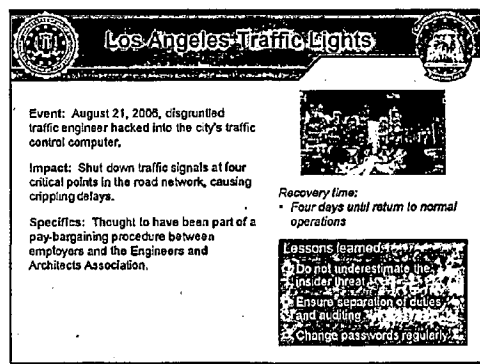
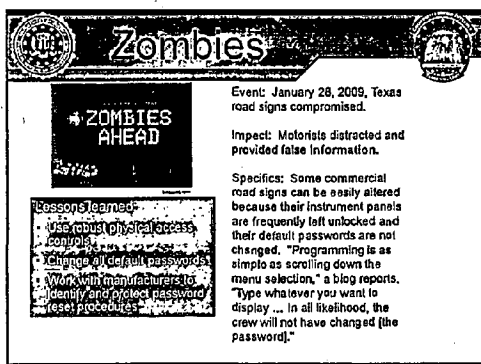
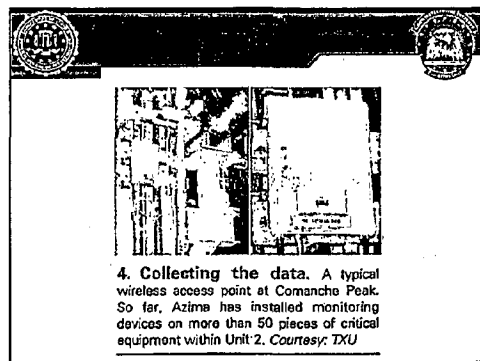


Computer Intrusions

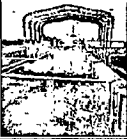


- Intruders gain access by various methods such as using exploits for a particular computer system or exploiting a weak account password. (Goal is to gain root or administrator privileges)
- Results
 - Theft and/or destruction of sensitive data
 - Computer network damage
 - Control of computer for other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

[illegible][illegible]



Maroochy Waste Water



Event: March 2000, more than 750,000 gallons of untreated sewage intentionally released into parks, rivers, and hotel grounds.

Impact: Loss of marine life, public health jeopardized, \$200,000 in cleanup and monitoring costs.

Specifics: SCADA system had 300 nodes (142 pumping stations) governing sewage and drinking water.

Lessons learned:

- Suspend all access after termination
- Investigate anomalous system behavior
- Secure radio and wireless transmissions

Davis-Besse Nuclear Power Plant



Event: August 2003, Slammer worm infects plant.

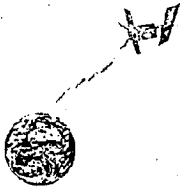
Impact: Complete shutdown of digital portion of Safety Parameter Display System (SPDS) and Plant Process Computer (PPC).

Specifics: Worm started at contractors site.

Lessons learned:

- Secure remote (trusted) access channels
- Ensure defense-in-depth strategies with appropriate procurement requirements
- Critical patches need to be applied

NASA Space Station



Event: Aug. 2008, Viruses intended to steal passwords and send them to a remote server infected laptops in the International Space Station (again).

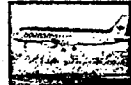
Impact: Created a "nuisance" to non-critical space station laptops.

Specifics: The virus did make it onto more than one laptop—suggesting that it spread via some sort of intranet on the space station or via a thumb drive.

Lessons learned:

- Due to the human factor, there is no true airgap (e.g. thumb drives, laptop connections, modems, VPN, CD/DVD, etc.)

Malware implicated in fatal Spanair plane crash



Event: October 12, 2008, a Boeing 737-800 aircraft crashed on takeoff from Madrid, Spain, minutes after departure.

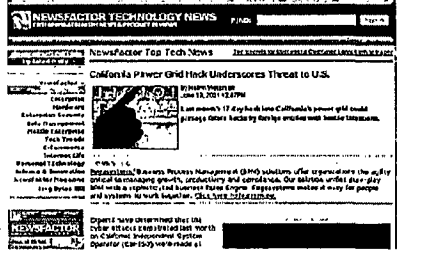
Impact: The crash resulted in the deaths of 154 people.

Specifics: The investigation found that malware had infected the aircraft's flight deck systems, causing the autopilot to disengage and the aircraft to lose control.

Lessons learned:

- The investigation found that the malware was likely introduced via a USB drive.
- The aircraft's flight deck systems were not adequately protected from malware.
- The investigation found that the aircraft's flight deck systems were not adequately protected from malware.

California Power Grid Hack Underscores Threat to U.S.



Event: A hacker group called 'The Dark Army' claimed to have hacked into the California Power Grid.

Impact: The hack caused a power outage in parts of California.

Specifics: The hacker group claimed to have accessed the grid's control systems and caused a power outage.

Lessons learned:

- The investigation found that the grid's control systems were not adequately protected from hackers.
- The investigation found that the grid's control systems were not adequately protected from hackers.

Who Are They



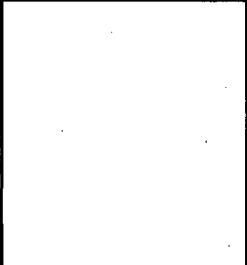



Cyberterrorists

- Evolution of existing terrorist groups
 - Tech-savvy members or new recruits develop cyber capability, or
 - Group hires hackers to conduct attacks
- Emergence of new terrorist groups
 - New group has interest in cyberterror – develops skills or hires hackers
- Individuals or groups with hacking skills
 - Operate independently
 - May align themselves with terrorist networks and objectives
 - May have insider help

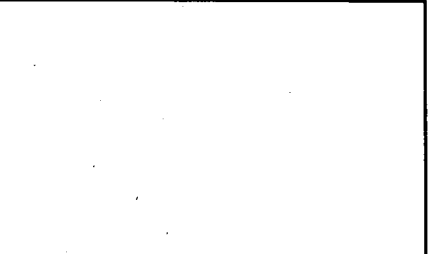



Cyber Jihadists



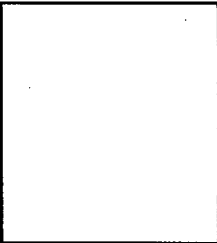

b7E



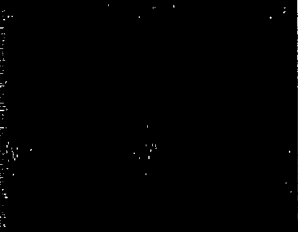



Digital Pearl Harbor ???




b7E

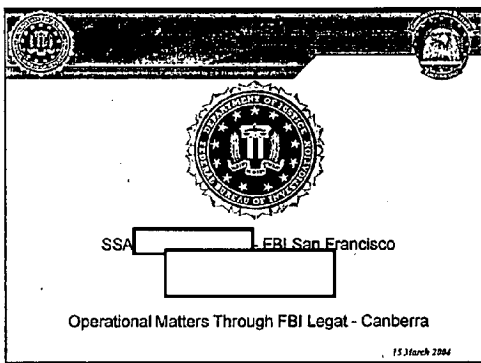





QUESTIONS ??





b6
b7C
b7E