Cyberterrorism: The Bloodless War?

2

Pat Mcgregor Chief Information Security Architect Intel Corporation 3 October 2001 The threat of terrorist attacks against **U.S.** citizens and U.S. interests around the world has become the nation's most pressing national security issue. ... This aggression may include cyber attacks by the terrorists themselves or by targeted nation-states.



Even more likely are cyber attacks by sympathizers of the terrorists, hackers with general anti-US or anti-allied sentiments, or thrillseekers with no particular political motivation.

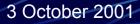
Cyber Attacks During the War on Terrorism: A Predictive Analysis Dartmouth Institute for Security Technology Studies

What Do We Know?

Cyber attacks immediately follow physical attacks Cyber attacks are increasing in volume, sophistication, and coordination Cyber attackers are attracted to highvalue targets Many, if not most, targets would probably be commercial computer and communications systems

Cyberwar Strategies

The basic elements are: Hacking Virus writing Electronic snooping Old-fashioned human spying Mass disruption can be unleashed over the internet, but Attackers first must compromise private and secure networks



InfoWarriors are not Scrip Kiddies

Funded by foreign military organizations and terrorist groups

Likely to have more people and deeper pockets
 Can devote more resources – people and time

- They can crack systems that might withstand casual assault
- Likely to be more experienced
 - Will use more sophisticated tactics

Serious IW attackers would not reveal their activities until it is absolutely necessary

Commercial Sector a Key Target

Communication systems News organizations **Telephony suppliers** Corporations Component suppliers (boots, food, radios, etc.) • Civilian consulting companies Financial institutions Government funds tied up in commercial banks Healthcare industry • Pharmacies, hospitals, clinics Drug companies (vaccines, antibiotics)

But Companies Not the Only Targets

Power grids

For 11 days in Feb 2001, a development server at cal-ISO electricity exchange was left connected to the internet and was being quietly hacked

Transportation systems

 "A foreign adversary could significantly hinder U.S. Forces in reaching, say, the Persian gulf or Taiwan straits by attacking the computers at commercial harbor facilities used to ship ammunition or the air traffic control system that would be needed to support and airlift personnel and supplies" (Bruce Berkowitz)

Water authorities

Why Use Cyber Warfare?

Low barriers to entry – laptops cost a lot less than tanks Complex societies are dependent on computers and networks Computer disruption has economic, logistical, and emotional effect Paralysis caused by computer outages levels the playing field for less-wellequipped countries

What Can We Do?

Go on the defensive *now*Educate senior management on risks of cyberwarfare Make infosec a top priority Beef up your security technology

- Insist on flawless execution: compliance to security standards in all areas
- Work with other companies, government agencies
 - NIPC
 - IT ISAC
 - SAINT

Some Specifics: Be Prepared

Maintain high alert & vigilance Update OS and applications regularly Enforce strong passwords "Lock down" systems Keep anti-virus software installed and up-to-date Employ intrusion detection systems and firewalls

Questions?



Cyberterrorism/P McGregor

Thank you!

intel

Pat McGregor pat.mcgregor@intel.com +1 916 356 3558

3 October 2001

Cyberterrorism/P McGregor

Selected Sources

 Berkowitz, Bruce, "Information Warfare: Time to Prepare." *Issues in Science and Technology*, Winter, 2000. http://www.nap.edu/issues/17.2/berkowitz.htm

- Gaudin, Sharon, "Protecting a net in a time of terrorism", Network World, 09/24/01. <u>http://www.nwfusion.com/archive/2001/125631_09-24-2001.html</u>
 - "Cyber Attacks During the War on Terrorism: A Predictive Analysis." Dartmouth Institute for Security Technology Studies.

http://www.ists.dartmouth.edu/ISTS/counterterrorism/cyber_attacks.htm

- Bickers, Charles, "Innovation, Cyberwar, Combat on The Web". Far Eastern Economic Review, August 16, 2001
- Risks Digest. <u>http://catless.ncl.ac.uk/Risks</u>