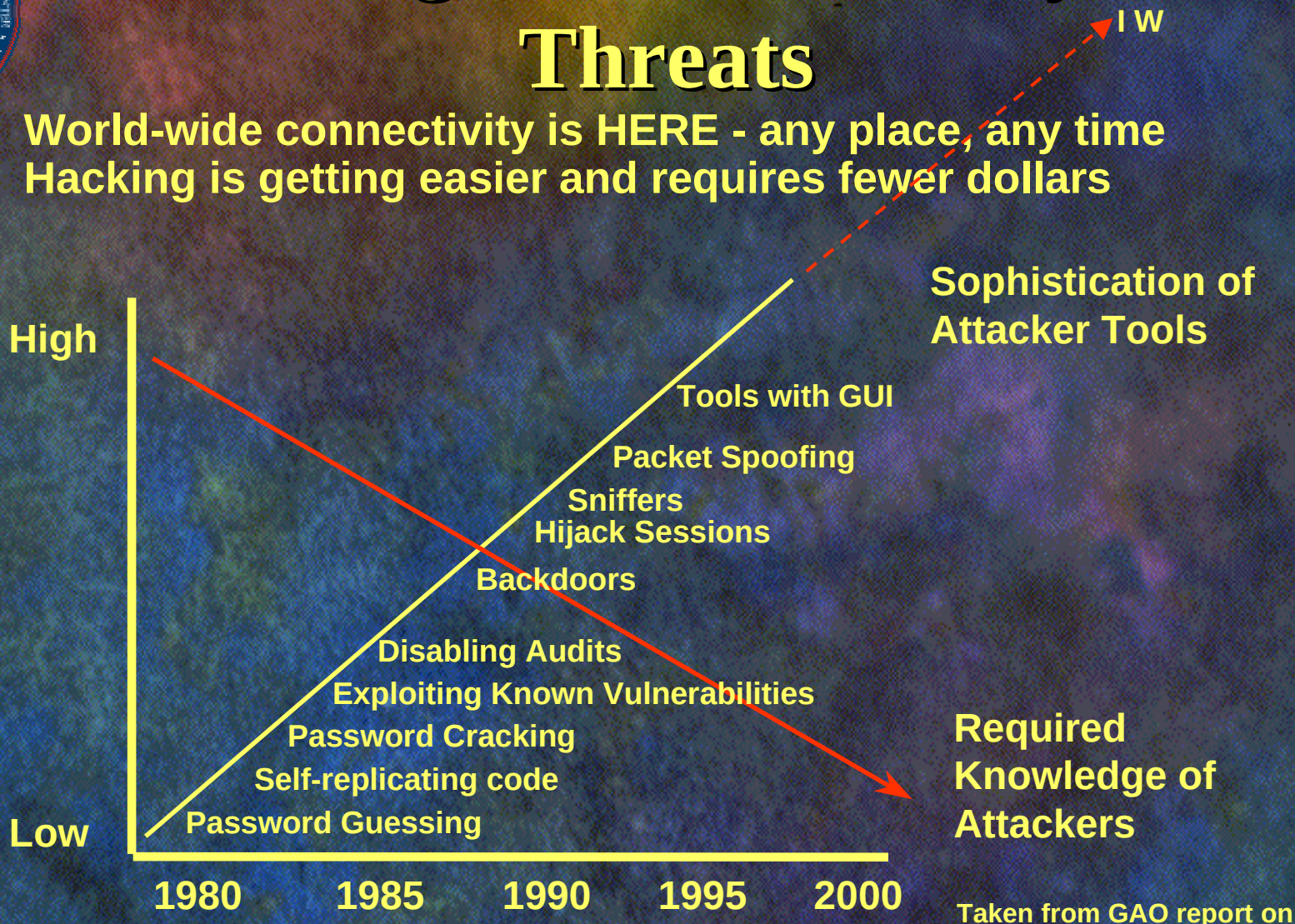
Threats to the US Electric Power Infrastructure:

October 1999 - October 2000

FOR OFFICIAL USE ONLY

Growing World-Wide Cyber Threats

World-wide connectivity is HERE - any place, any time
Hacking is getting easier and requires fewer dollars



Taken from GAO report on DOD security

Any Country, Group, or Individual

Attractiveness of Electric Power As A Target

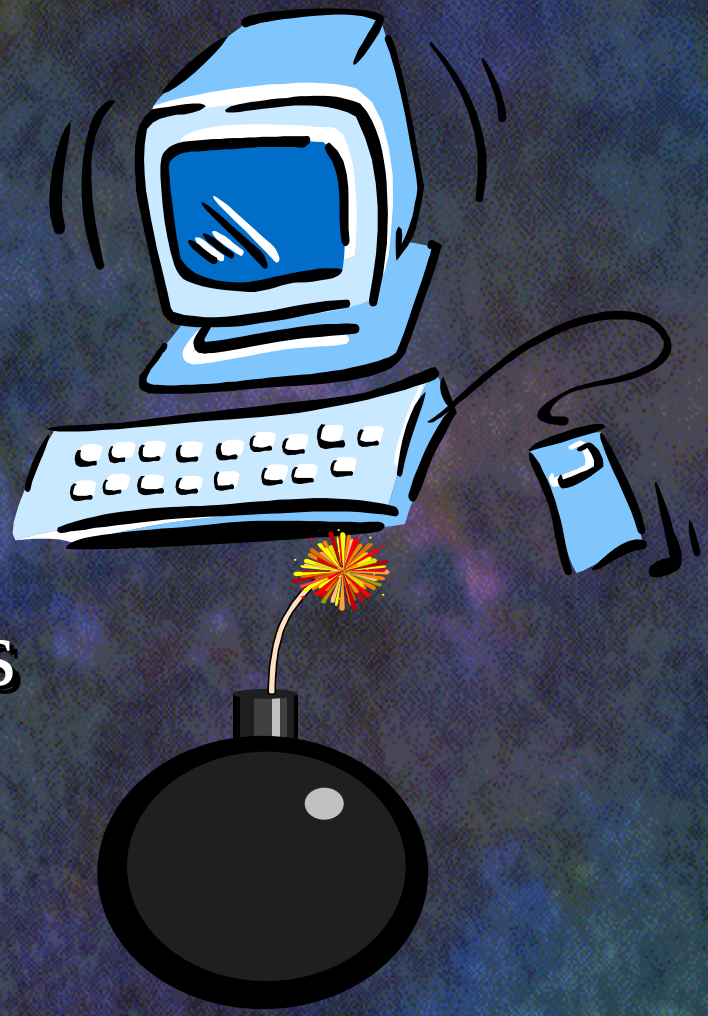
- Critical support to economy, national security, and public well-being
- Possible conduit to specific national security or economic targets
- Possesses symbolic value as a target
- Possesses monetary value as a target
- Conduit to other critical infrastructures

Example: World-Wide Cyber Threat Against One Power Company

- Target: company's Internet-connected computers
- Exploits: ~230,000 unauthorized attempts during one month to connect to company computers via the Internet
  - Over 86,000 attempts originated from China alone (largely searches for proxy servers)
- Impact: None; all attempts were blocked and logged at company's firewall

Potential Adversaries

- Hackers
- Criminals
- Insiders
- Economic Competitors
- Terrorists
- Nation States



Adversary: Hackers

Example : Unauthorized use of power grid manager's server for interactive game playing

- Target: Grid manager's email list-server
- Exploit: Unauthorized game installation resulting in theft of bandwidth and disk storage space
- Impacts: degraded market function, grid management, anomalous system behavior

Adversary: Insider

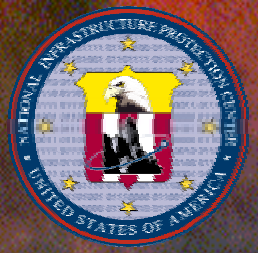
Example: Alleged sabotage-improper mix of pellets in fuels fabricated for commercial nuclear power plants

- **Target: Nuclear fuel production plant**
- **Exploit: Mixing disproportionate % of "erbium pellets" in uranium fuel**
- **Impact: Threat event-financial loss to plant during shutdown for investigation**

Adversary: Criminals

Example: Deliberate cut of fiber optic line supporting SCADA control and other essential utility communications

- Target: System Operator/electric utility
- Exploit: Physical cut/theft of fiber optic line
- Impact: Loss of telecom needed for system operations (e.g., SCADA, radio & voice communications)



Adversary: Nation State (Information Warfare ?)

Example: DOS attack against power grid manager's firewall

- Target: Firewall belonging to a power pool manager
- Exploit: DOS attack
- Impacts: Degraded control communications degrading ability to control operations on the grid