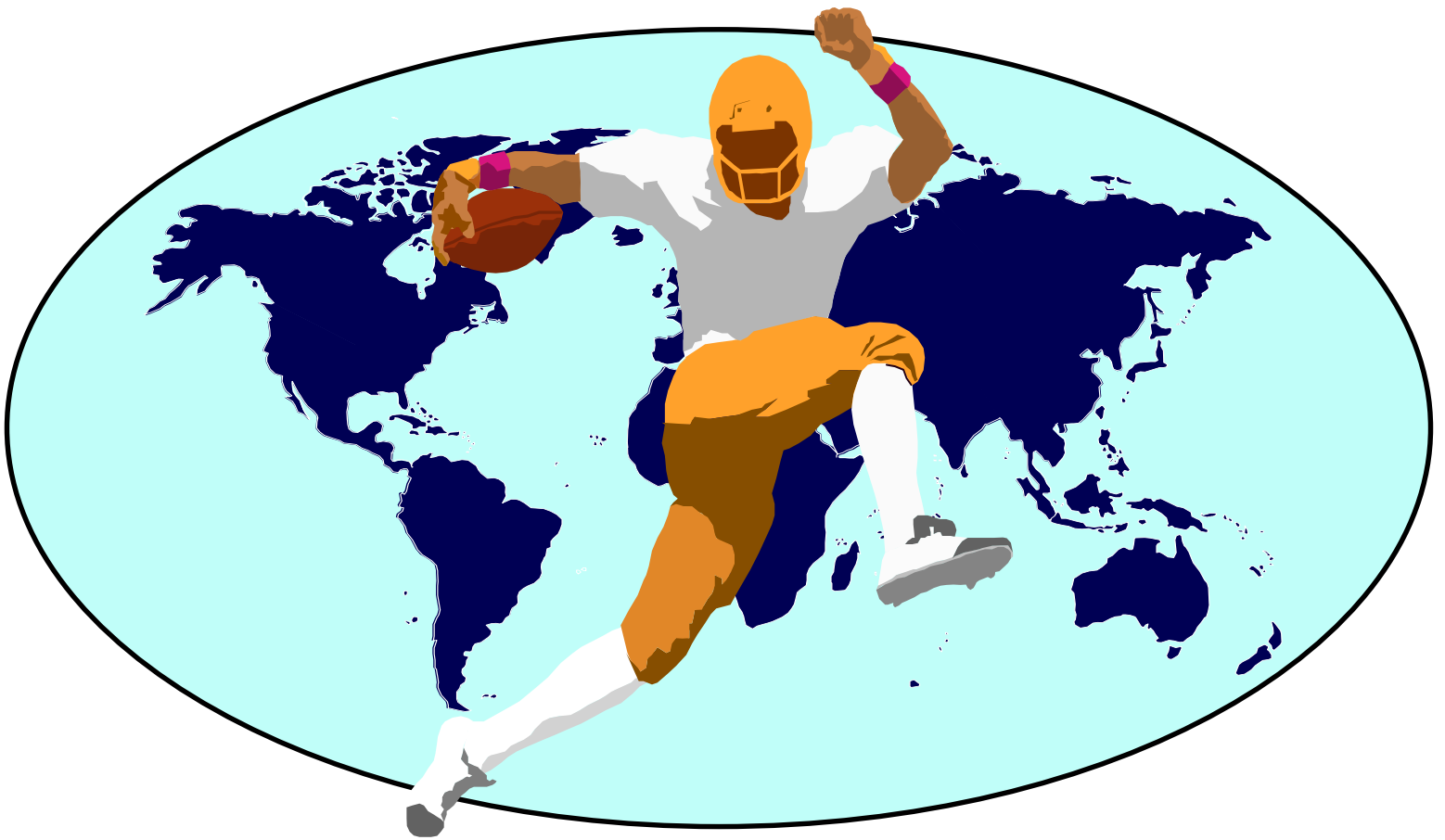
Exercise ELIGIBLE RECEIVER 97



ELIGIBLE RECEIVER Program

- ***ELIGIBLE RECEIVER***
  - An exercise series
  - Directed by the *Chairman of the Joint Chiefs of Staff*
  - Designed to test DOD *planning and crisis-action capabilities*
- ***ELIGIBLE RECEIVER 97*: *Conducted 9-13 June 1997***
  - First large-scale exercise designed to test our ability to respond to an ***attack on our information infrastructure***
  - Also evaluated ability to work with other branches of government to respond to an ***attack on National Infrastructure***

ELIGIBLE RECEIVER 97 revealed:

- ***Significant vulnerabilities*** in US Defense Information Systems
- Deficiencies in responding to a ***coordinated attack*** on National infrastructure and information systems

ELIGIBLE RECEIVER 97 Participants

- Department of Defense
- The Joint Staff
- Military Services
- Combatant Commands
  - *US Atlantic Command*
  - *US Pacific Command*
  - *US Space Command*
  - *US Special Operations Command*
  - *US Transportation Command*
- National Security Agency
- Defense Information Systems Agency
- National Security Council
- Department of State
- Department of Justice
- Department of Transportation
- Defense Intelligence Agency
- Central Intelligence Agency
- Federal Bureau of Investigation
- National Reconnaissance Office

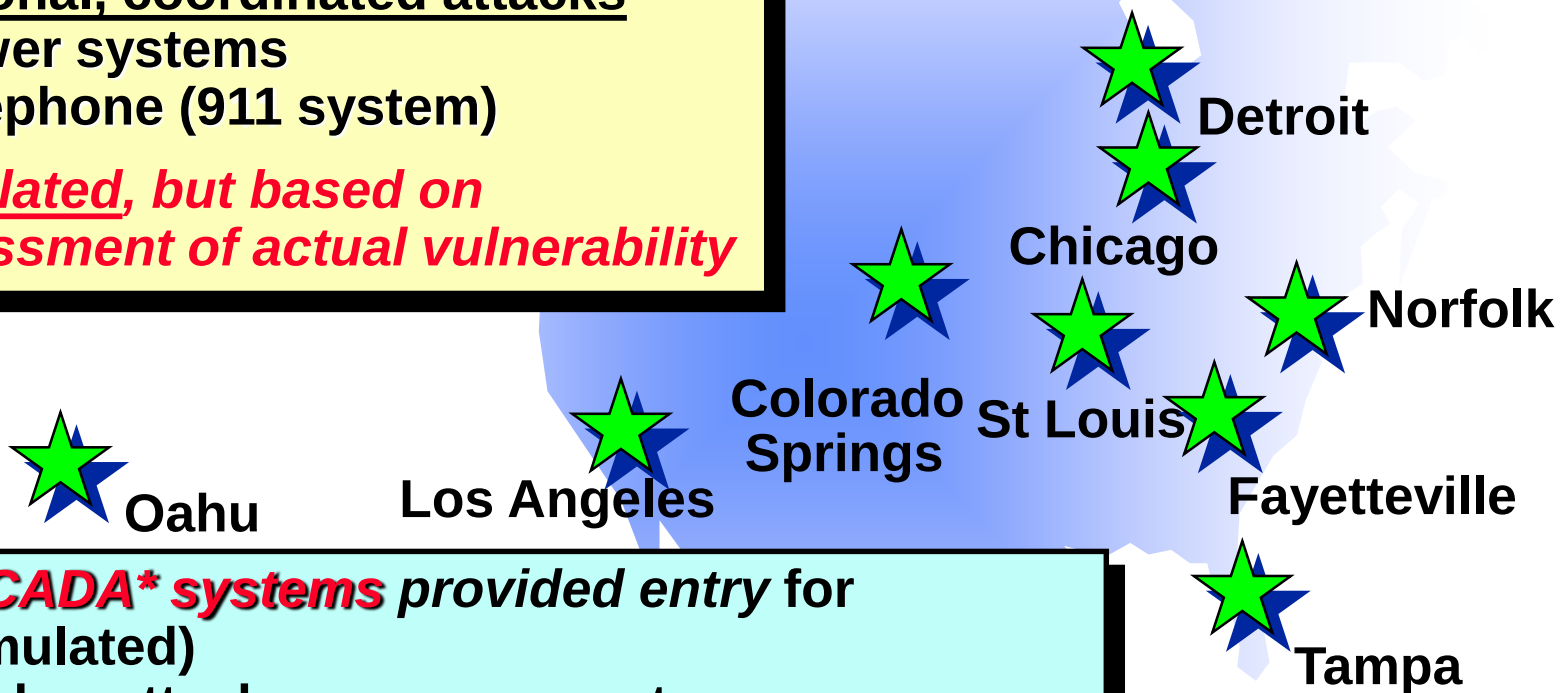
Attack Phases

- **Phase I: *National Infrastructure Attack* (Simulated)**
  - **Against portions of *national infrastructure* (power and communications systems)**
  - **Designed to cause *public pressure* for action**
  - **Simulated, but *based on assessed vulnerabilities***
- **Phase II: *Defense Information Attack* (Actual)**
  - **Targeted key Defense information systems**
  - ***Actually intruded into* many computer systems**
  - **Exploited *actual vulnerabilities* of our system**

Power and Telecom Attack

Regional, coordinated attacks
- Power systems
- Telephone (911 system)

Simulated, but based on assessment of actual vulnerability



- ***SCADA* systems*** *provided entry* for (simulated) cyber attacks on power systems
- Overloading phone systems ***disrupted communications***
- ***Public sources*** provided the knowledge

**Supervisory Control and Data Acquisition*

Computer Network Attack Plan

PRIORITY TARGETS

- National Military Command Center
- Combatant Commands
  - *Pacific Command*
  - *Space Command*
  - *Transportation Command*
  - *Special Ops Command*
- Defense Logistics Agency

TYPES OF ATTACK

- Intruded into Computer Systems
- Denied Service
- Changed Data
- Removed Data
- Interrupted E-mail
- Disrupted phone service

All attacks used commonly available "hacker" tools

ELIGIBLE RECEIVER 97- Key Observations

❶ Defense and National Information Infrastructures are ***highly interdependent***

❷ National decision-making structure and coordination processes are ***unresponsive to speed of attacks***

❸ No structure or process exists to ***coordinate DoD defense***

- No ability to interface with rest of US government, allies and private sector

❹ ***"Indications and Warning"*** process is ***inadequate***

❺ Little capability exists to ***detect or assess cyber attacks***

❻ Characterization and attribution of attacks is ***very difficult***

❼ Many ***legal questions*** must be addressed

❽ ***Poor information / operational security practices*** contributed to vulnerabilities

"This is Not an Exercise"

An Actual Attack on DOD Computer Systems occurred during February 1998

Code Name:

SOLAR SUNRISE

SOLAR SUNRISE

- ***SOLAR SUNRISE*** **incident occurred from 1 to 26 February 1998**
  - **DOD computer systems were *systematically attacked***
- **Attack pattern indicative of *preparation for a coordinated attack* on Defense Information Infrastructure**

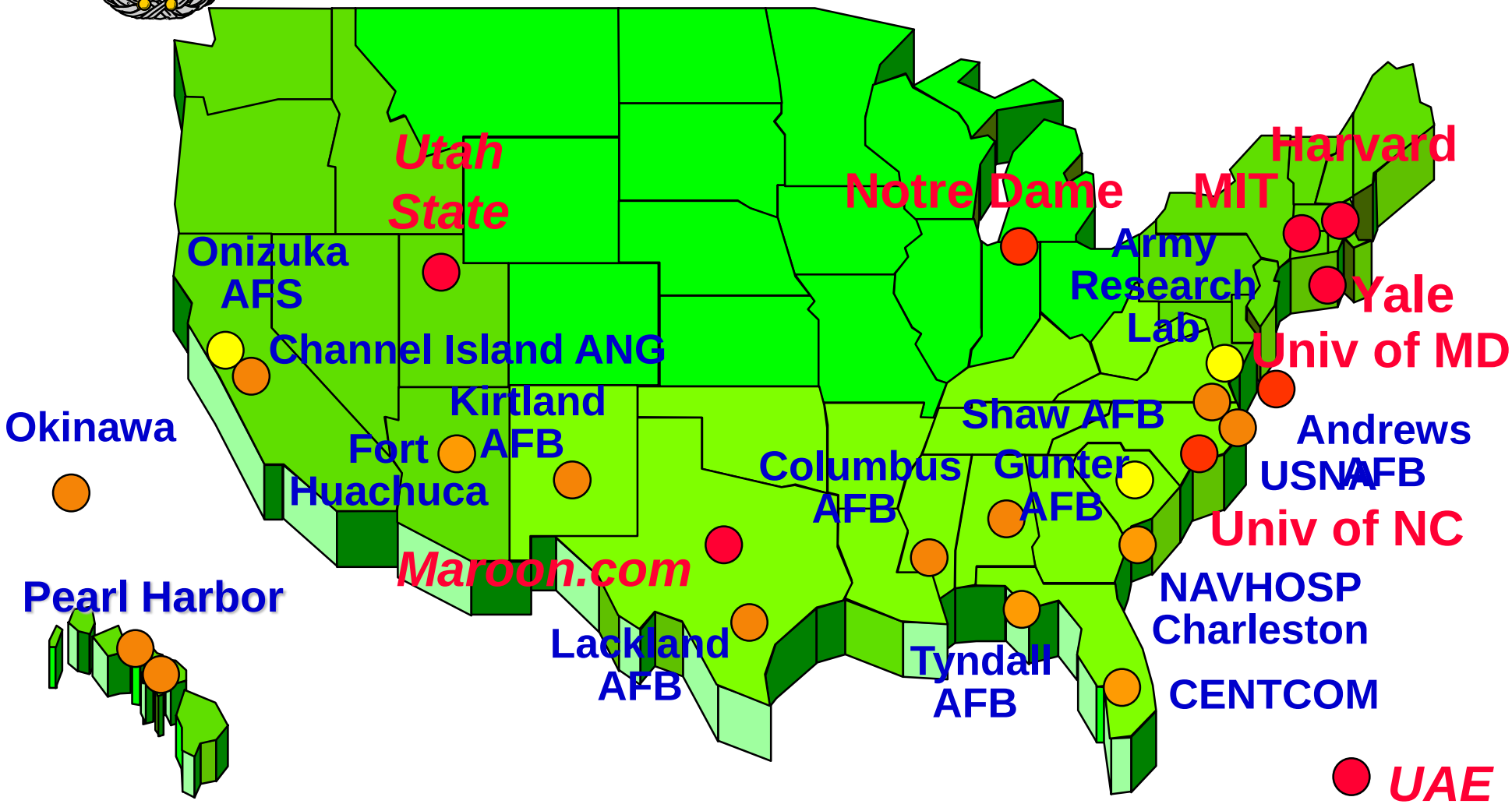
SOLAR SUNRISE - Attack Profile

- Attacks targeted DOD network ***Domain Name Servers***
- Exploited ***well-known vulnerability*** in ***Solaris Operating System***
- Attack profile

1 - ***Probe*** to determine if vulnerability exists in server
2 - ***Exploit vulnerability*** to enter computer
3 - ***Implant program*** to gather data
4 - Return later to ***retrieve collected data***

- ***Numerous attacks*** followed same profile

Further Indications of Activity



The Basis of Our Concern

- Attacks were ***widespread*** and appeared to be ***coordinated***
- Attacks ***targeted key parts of defense networks***
- Attackers attained *many* network passwords
- Could not characterize or attribute attacks
  - ***Potential*** connection with impending ***operations in Gulf?***
- ***Key support systems*** depend on unclassified network
  - Global Transportation System
  - Defense Finance System
  - Medical, personnel, logistics
  - Official unclassified e-mail

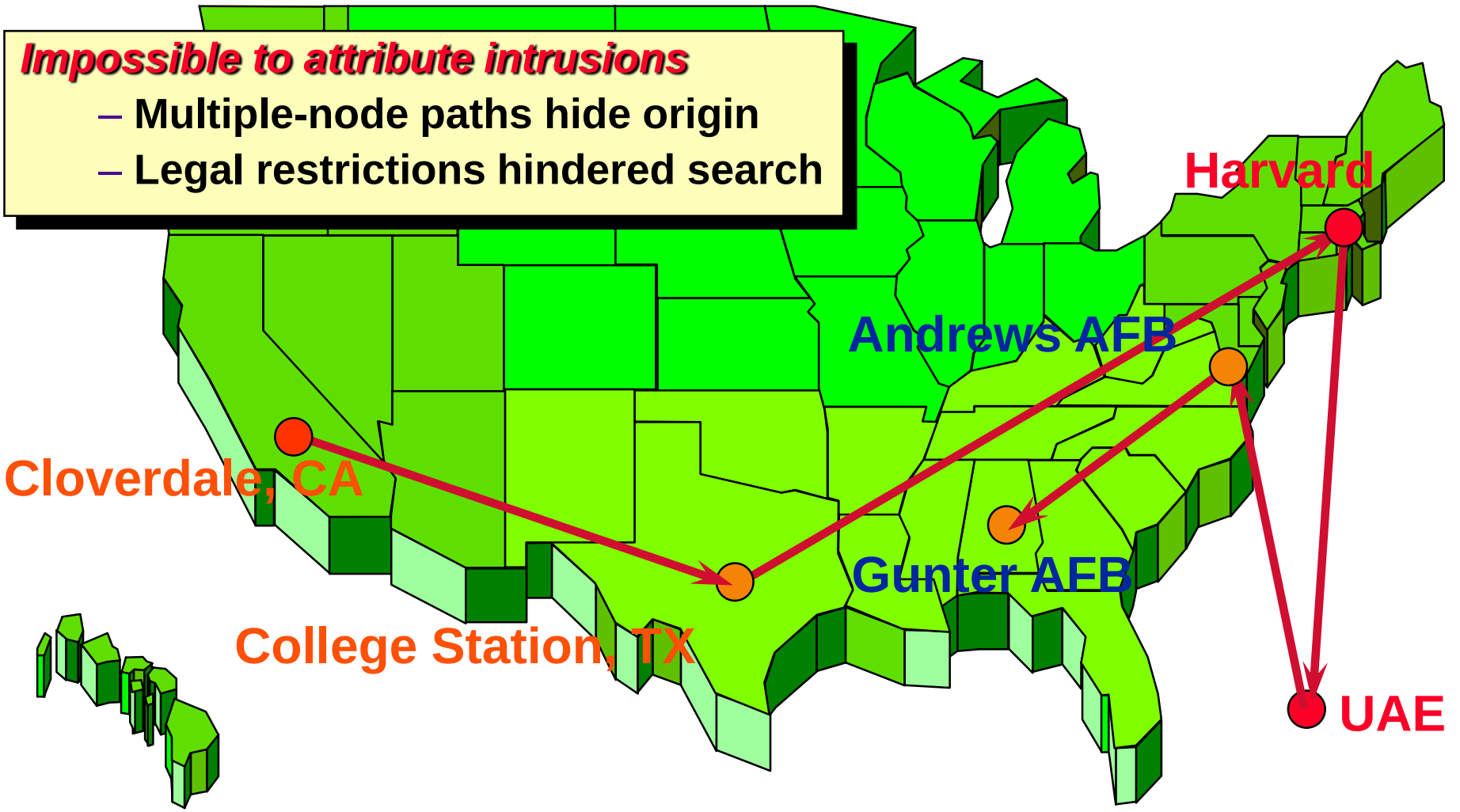
Characterization

- **Important to establish *intent***
  - ***Worst-case*: *coordinated strategic attack***
    - **Coordinated with Gulf activities?**
    - **Possible preparation for Information attack**
  - ***Possible*: *terrorists, criminals***
    - **No intelligence information to support**
  - ***Most likely*: *"Hackers"***
    - **Some characteristics of hacker games**
    - **No damaging exploitation of systems or data**
- **Forensic analysis helps, but *slow* and *resource-intensive***

Attribution Challenges

Impossible to attribute intrusions

- Multiple-node paths hide origin
- Legal restrictions hindered search



DOD Defensive Actions

- Increase DOD awareness: ***24-hour watch***

- Identify and patch *systems at risk*
- Install ***intrusion detection systems*** on key nodes

- Analyze data to *assess attacks* and develop leads
- Dispatch ***Emergency Response Teams*** to hottest sites to assist fixes
- Assess status of systems; fix and *begin cleanup*

- Form Red Team to ***reverse engineer attacks***
- Plan for degradation/loss of network

- Share data with ***private sector***
- Team with ***law enforcement agencies***

SOLAR SUNRISE Summary

- **Confirmed *ELIGIBLE RECEIVER* findings**
  - **Legal issues remain *unresolved***
  - **No effective *Indications and Warning* system**
  - ***Intrusion detection systems* insufficient**
  - **DOD and Government *organizational deficiencies hinder* ability to react effectively**
  - **Characterization and attribution problems remain**
- **Need to establish standing *response team***
- **Increased detection capability forces new choices**
- ***High interest, high visibility* issue**
  - **Increases pressure for an *quick response***

The *"ENEMY"*

- **On 26 Feb, FBI served warrants on the *attackers:* *two 16 year old boys in California***
- **Tools were only *moderately sophisticated***
- **May have been tutored by *foreign mentor***
  (Note: On 18 March, Israeli police in Jerusalem arrested *"The Anaylzer"* for his role in DOD intrusions)
- **Hacker 1: *"We did it for the power"***

What can *determined and sophisticated* attackers do?

BACKUP