DOT&E Support for Joint Vision 2020 via Information Assurance Testing

21 March 2001

Mr. Lee Frame
Acting Director, DOT&E

Our Reason for Being Here

- **US Defense Trends**
  - Increasingly High-tech
  - Less manpower... More reliance on computer networks
- **The Threats**
  - Standard or Asymmetric
  - Nation States, Rogue Elements, Individuals
- **The Law**
  - FY 00 Congressional Language
  - The FY 01 Defense Authorization Act (P.L. 106-398, Subtitle G, 30 Oct 2000) requires conduct of annual IA program reviews
- **The DoD Response**
  - DOT&E on-going test and evaluation (T&E) effort
  - GISRA-IPT (April 01 report to Mr. Money; DoD Oct 01 report to Congress)

Threats and Targets

- **Entities**
  - Nation States… “friendly” and otherwise
  - Sub-national and Transnational Groups
  - Professional “Crackers”
  - Disgruntled Insiders
  - “Amateur” Hackers
- **Techniques**
  - Perform Information Warfare (theft, forgery, cyber plagues...)
  - Computer Network: Attack and Defend (CNA and CND)
  - Full Spectrum of Attacks and Toolkits
    - » For Sport, to Commit Crime, or to affect National Security
    - » From Electronic Warfare… to Social Engineering
- **Targets: Civil and Military Critical Infrastructure**

Recent IW Headlines

Bin Laden: Steganography Master?
Wired, 7 Feb 01

Hacker Hits on Pentagon Computers Up 10 Percent This Year
Washington Post, 9 Dec 00

Analyst Warns of China's Aggressive Approach to Info Warfare
Inside the Pentagon, 30 Nov 00

Moonlight Maze: Russia Says Spies Not Linked to U.S. Computer Raids
Reuters, 7 Oct 99

E-Commerce: FBI Warns of Organized Computer Hacker Groups
Reuters, 8 Mar 01

Naked Wife Virus Hits Computers
Associated Press, 7 Mar 01

Companies, Feds Team to Stop Hackers
Associated Press, 17 Jan 01

Malware Mahem: Viruses by the Numbers
Information Security, Oct 00

The Threats are Busy... and Affect Us All

Anatomy of a Hack

Methodologies

- Footprinting
- Scanning
- Enumerating
- Access-Gaining
- Pilfering / Tampering
- Denial of Service
- Escalating Privileges
- Back Door Creation
- Track Covering

Techniques

- Search Engines
- War-Dialing & Pinging
- Account ID-ing
- Eavesdropping
- Social Trickery/Extortion
- SYN Floods; Viruses
- Brute Force Cracking
- Rogue Acct's - Trojans
- Log Clearing

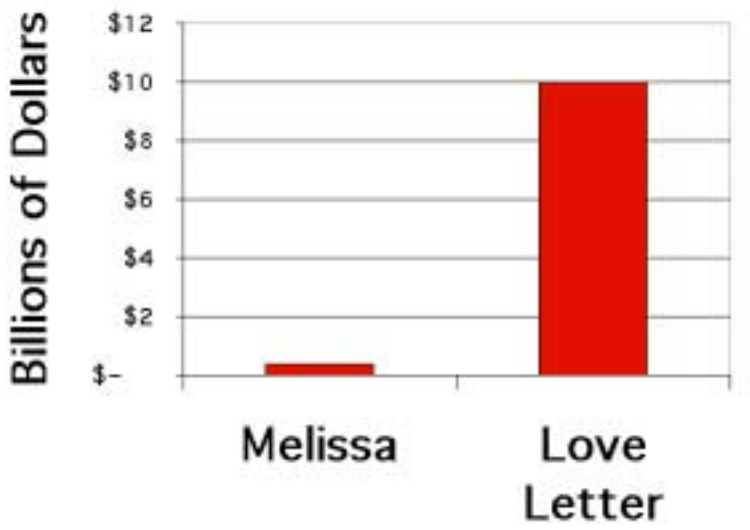
Information Warfare Examples

- **Military Examples**
  - Gulf War Episodes
  - Solar Sunrise
  - Moonlight Maze
  - Eligible Receiver
- **Civil Examples**
  - Kevin Mitnick (phones, networks, data)
  - Operation Sun Devil (SW Hackers; FBI and Secret Service)
  - Operation Moon Angel
  - Viruses: Melissa, Love Bug, Naked Wife...

Some Hacking Statistics

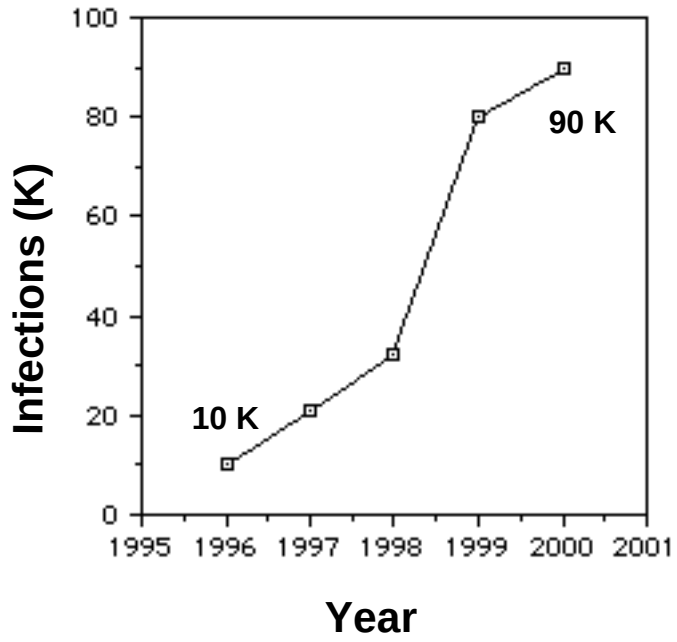
Damage & Lost Productivity

Source: *Information Security* 10/00



Monthly Rate of Infected PCs

Source: *Information Security* 10/00



A Serious Impact on Both Government and Industry

Information Assurance Motivation

- Information superiority is key goal for JV2020
- US becoming critically dependent on information vulnerable to attack
- Formalized operational evaluation of all systems makes users aware of vulnerabilities
- Quick response was to formalize test policy for information assurance that was lacking

Policy Development

- Multiple IA policy workshops conducted with Services and Agencies to start defining policy
- Some concerns:
  - How do we test this? Led to guidelines development
  - New requirement without additional funding?
- Congressional language in FY2000 DoD funding bill mandated IA testing
- Policy signed 17 November 1999

Guidelines Development

- During policy development, Services expressed need for defined IA metrics and common guidelines for implementation
- DOT&E organized another series of workshops and meetings with Service IA centers and testers to define metrics and guidelines
- IA Metrics and Guidelines signed January 2001

Next Steps

- **Policy Signed in 1999**
  - Was a DoD "First Step" in Information Assurance
  - IA Testing Must be Accomplished — Today
- **Are More Dependent on Computers, Networks, and Information Flow**
- **Information Assurance is more than Defensive Cyber War… It is Access**
- **Other Threats will Require Further Assessment**
  - RFI; Hi-Powered Microwave; Physical Destruction; Information Intercept
  - Advanced "Social Engineering"

What We Hope to Accomplish Together

- **Promote cross-pollination among Services and Industry**
- **Review DoD Policy implementation**
  - *Case Studies*
  - *Lessons Learned*
- **Spread the word within DoD test and acquisition communities**
- **Define and Better Understand the Challenges**
- **Identify what else we need**
  - **Better Information?**
  - **More Expertise?**
  - **Additional Education?**
  - **What does the Future hold?**