PITAC National Security Panel

PITAC Meeting

February 8, 2001

Carrying Out the Agenda

- The Panel believes a major effort is necessary to address the effective and innovative use of IT for national security.
- The Panel will consider what shape and form it might take, how it could be put in place and a range of cost vs benefit evaluations.
- The Panel plans continued interactions with the appropriate parties in the government and private sector

Background

- Preliminary Teleconference in December
- Meeting on Friday, January 5th, 2001
- Meeting on Wednesday, February 7th, 2001
- Presentations by:
  - George Cotter et al., NSA - Supercomputers
  - Shankar Sastry, DARPA - DSB Study on Defensive Information Operations
  - Jeffrey Hunker, NSC - Critical Infrastructure
  - Linton Wells, C3I - Transition Briefing on Information Superiority

Proposed Charter

- Identify long-term IT research issues & opportunities to enhance national security in a networked world; address both Defense and private sector aspects.
- Describe possible Testbeds and Scenarios for demonstrating advanced IT research results and technologies for enhanced national security
- Look to the future; do not focus on existing programs or their vulnerabilities and weaknesses in findings and recommendations.

Consider Related Studies

- Most Recent is the Rudman-Hart report
- Other reports previously issued or in various stages of preparation including those from the Defense Science Board
- National Plan for Protection of Critical Infrastructure (PDD 62 & 63)
  - Cyber-CIO at Gov't Level, ISACs, Interworking with Industry Sectors
- Panel agreed to keep the report unclassified

Tentative Schedule

- Additional Inputs through April
- Preliminary First Draft in Spring (May-June)
- Coordinate over the Summer - revise and iterate
- Prepare Final Report - September

Issues & Concerns

- Four Different but Related Concerns
  - National Defense
  - Orderly Society
  - Competitiveness
  - International Relations
- Formulating the Research Agenda
- Testbeds, Prototypes, Pilots, Experimentation, Infrastructure

Initial Focal Points

- Catastrophic Infrastructure Attacks
  - Detect, Defend, Maintain during attack
  - Coalition of heterogeneous systems
  - Dynamic Adaptation
- Cyber-Visibility
  - Track unfolding events, intruders
  - Predict ramifications
  - Technology “Eyes and Ears”
  - Characterization of data & events

Initial Focal Points

- Reconstitution
  - Backup monitoring & oversight
  - Information, Systems, Connectivity
  - Rapid Status Feedback
- Other Major Areas
  - Hackers, Cybercrime & Cyberterrorism
  - Wireless Vulnerabilities
  - Privacy & Security
  - Verification & Authenticity

Touchstones

- Viruses - worldwide coordination in combatting
- Snooping, Sniffing, Squatting, and Spamming+
- Detecting & Debugging - e.g. bogus e-contracts
- Integrity - e.g. Financial Transfers
- Validity of Ids, Certificates, and Data Structures
- Command authenticity, event replay, postmortems
- Critical Information retention, visualization & handoff

Being Effective

- How to insure the research and testbed findings and recommendations are on-target for the parties who have the relevant missions in Defense and elsewhere.
- Concept Push vs Concept Pull!

Operational Management

- Taking Charge
  - Pre-arranged lines of authority? for what? Dynamic adaptation during crises?
  - Who decides? How does coordination occur?
  - Formalized Country-Country Processes? Levels
- International Cooperation
  - Sharing research results
  - Managing interacting systems
  - Responding to developing situations