



**Defense Advanced  
Research Projects Agency**

**Dr. Anthony J. Tether  
DARPA Director**



# National Cyber Range

## National Cyber Range ACHIEVEMENT

STATUS QUO

- **Incremental technology focus**
  - COTS = Evolutionary advancement
- **Changing threat**
  - 1 billion potential attackers
- **Nation lacks**
  - Coordinated cyber research vision
  - Realistic testing environments
  - Quantifiable cyber programs benefits
- **National leaders lack confidence net-centric capabilities will be there when needed**



NEW INSIGHTS

- **United States needs:**
  - High-risk, paradigm-shifting cyber research programs
  - To evaluate results in a realistic, representative network environment
- **Unbiased, consistent testing provide ground truth and motivates new research vectors**



### MAIN ACHIEVEMENT:

- **Quantitative revolution in Nation's ability to conduct offensive & defensive cyber operations**
- **Persistent cyber range infrastructure**
  - Permits unbiased assessment of offensive and defensive capabilities and assess equities in a neutral environment
  - Allows realistic effects to be created and distributed to training/ test audiences
- **Potential lead-ahead research thrusts**
  - Formal evaluation framework and metrics
  - Verifiable programming languages
  - Asymmetry Inverted Environment
  - Revolutionary Cyber Situational Awareness (exploit complexity theory)

### HOW IT WORKS:

- Replicate complex network topologies found in current/future DoD weapon systems & operations
  - Includes WAN, satellite, MANET environments
  - 1K hosts simulating 10K nodes
- Emergent forensic data capture and analysis
- Dedicated adversary teams
- On-site technical support
- Consistent, verifiable testing accelerates transition & deployment of solution technologies

QUANTITATIVE IMPACT

- **Leap-ahead research and quantifiable assessment of cyber tools, processes, and architectures facilitates:**
  - Revolution in national cyber capabilities
  - Accelerates transition & deployment of developed technologies



END-OF-PHASE GOAL

- **FY08 -**
  - Assemble staffs
  - Develop research thrusts
  - Publish BAA
  - Host industry day
- **FY09 -**
  - Award contracts (Oct 08),
  - Initiate programs
- **FY10 -11**
  - Range IOC

# Vision



**Provide a realistic quantifiable assessment of the Nation's cyber research and development technologies to enable a revolution in national cyber capabilities and accelerate transition of these technologies in support of the President's Comprehensive National Cyber-Security Initiative (CNCI).**

**– The Range must provide:**

- (U) An interactive test suite to design, configure, monitor, analyze, and release tests
- (U) A tester toolkit/repository for recipes & architectures for reuse
- (U) Forensic data collection, analysis, and presentation
- (U) Realistically emulate human behavior and frailties
- (U) A realistic, sophisticated, nation-state quality red team.
- (U) On site, dedicated support for installation, troubleshooting, testing
- (U) Ability to emulate commercial and tactical wireless & control systems
- (U) A large pools of heterogeneous nodes as well as rapidly integrate new machines
- (U) The ability to integrate research protocols across or replacing the TCP/IP protocol stack
- (U) The ability to accelerate and decelerate relative test time
- (U) The ability to quantitatively evaluate technologies and architectures.
- (U) Encapsulation of tests, data storage and network – nothing spills across boundaries

**– The Range must support :**

- (U) Short and long-term research programs
- (U) Interactive and batch/non-interactive testing
- (U) The ability to test advanced capabilities against defensive tools



# What Did He Really Say?

“The National Cyber Range will allow classified and unclassified researchers to measure their progress

in either a classified or unclassified environment,

against appropriate threats with sufficient timeliness and accuracy,

to allow corrections and needed new capabilities to be determined.”

# Why Is It Needed?



- Over the ages scientific progress has been held back by the ability to make measurements at the level of the environment for which the scientific research was being done.
  - Telescopes, microscopes, particle accelerators, etc.
- The National Cyber Range is the measurement capability for cyber research in both classified and unclassified environments. Without it, research will be done in darkness and only stumble accidentally into the light.

