The Future of Cyber Experimentation and Testing

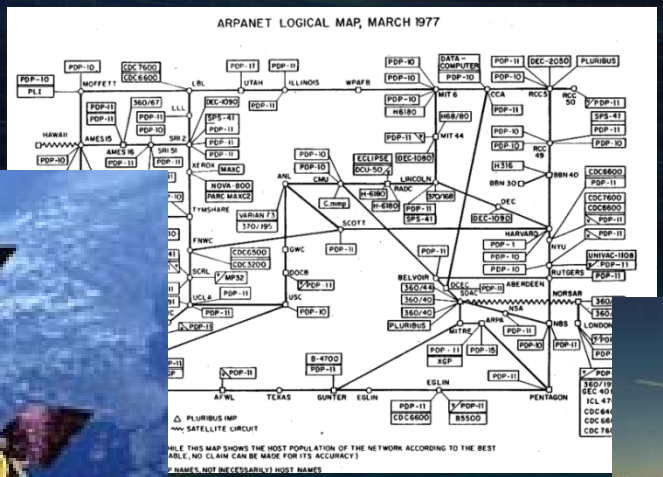
The U.S. NATIONAL CYBER RANGE

Michael VanPutte, Ph.D.
Program Manager

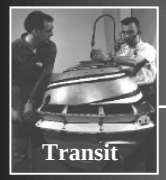
DARPA Mission

"… maintain the technological superiority of the U.S. military and prevent technological surprise from harming the U.S. national security by sponsoring revolutionary, high-payoff research bridging the gap between fundamental discoveries and their military use."

Since the very beginning, DARPA has been the place for people with ideas too crazy, too far out and too risky for most research organizations. DARPA is an organization willing to take a risk on an idea long before it is proven.



DARPA Accomplishments


Transit


VELA Hotel


ALTAIR


Mouse


ATACMS


Center for Monitoring Research


Stealth Fighter


Sea Shadow


GPS

1960

1970

1980


SATURN


M-16


Ground Surveillance Radar


ARPANET


Assault Breaker


JSTARS


TALON GOLD


MIMIC


Speech Recognition

1970

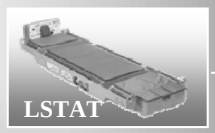

Command Post of the Future


Autonomous Ground Vehicles

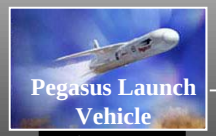

X-45


Mobile Robots


JSF Engine


LSTAT


Uncooled IR


Pegasus Launch Vehicle

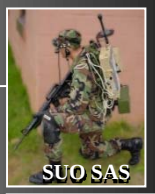

DARPASAT

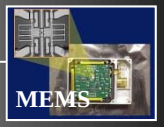
2000

1990

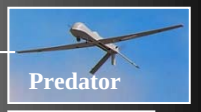

Phraselator


Exoskeleton


SUO SAS


MEMS


Global Hawk


Predator


BAT

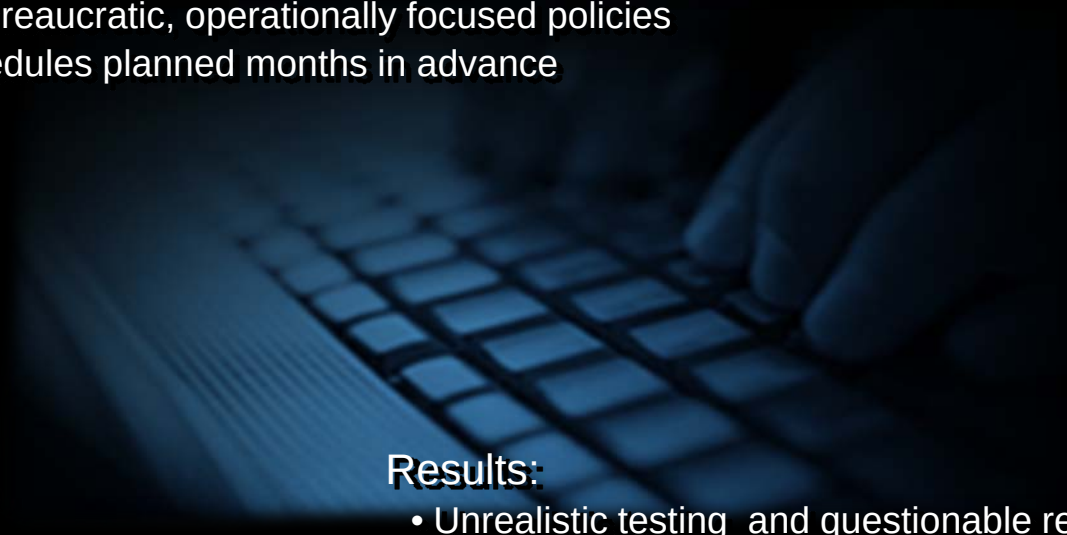

Advanced Cruise Missile


Taurus Launch Vehicle

Cyber Testing Today

Cyber operational community forced to deal with:

- Inflexible, expensive, special purpose testbeds
- Manual configuration and management
- Sacrificing test complexity for testbeds that are *"good enough"*
- Modifying systems under test to accommodate substandard, unrealistic testbed
- Constraining bureaucratic, operationally focused policies
- Rigid tests schedules planned months in advance



Results:

- Unrealistic testing and questionable results
- Slow research-to-operations transition loop
- Less functional production tools
- Expensive testing that restricts quantity of research performed
- Counter-threat research focused on today's threat

Operational vs Research and Experimentation

	Operational	Research
Mission	• Operational testing and demonstration; train today's warfighters	• Test and experimentation of radically new ideas from the research community
Goal	• Confirm or deny system meets today's stated warfighter requirements for the acquisition and fielding of warfighting systems.	• Advance understanding of the effects, consequences, and validity of potential systems on potential future environment
Systems Tested	• Production or production ready systems;	• Potential unstable research systems
Process	• Confirm or deny vendor claims within realistic, operational tests, assessments on current weapons, equipment, and doctrine	• Explore research space, drive future vision, create future requirements • Dynamic hypothesis generation and validation
Range Requirements	• Integrate current commercial & operational technology • Protect classified information • Technical support is focused on current commercial technology	• Integrate future technologies and protocols • Rapid test and testbed configuration • Rapid reset of tests to clean, new state for full-spectrum experimentation • Protect classified and proprietary information • Technical staff is more dynamic, interactive, and requires greater technical expertise

National Cyber Range

Strategic Technology Office

Provide a realistic quantifiable assessment of the U.S. cyber research and development technologies to enable a revolution in national cyber capabilities and accelerate transition of these technologies in support of the Comprehensive National Cybersecurity Initiative (CNCI).

Leap-ahead research and quantifiable assessment of cyber tools, processes, and architectures facilitates;

- Revolution in national cyber technologies
- Rapid technology development
- Accelerated deployment

Why Is It Needed?

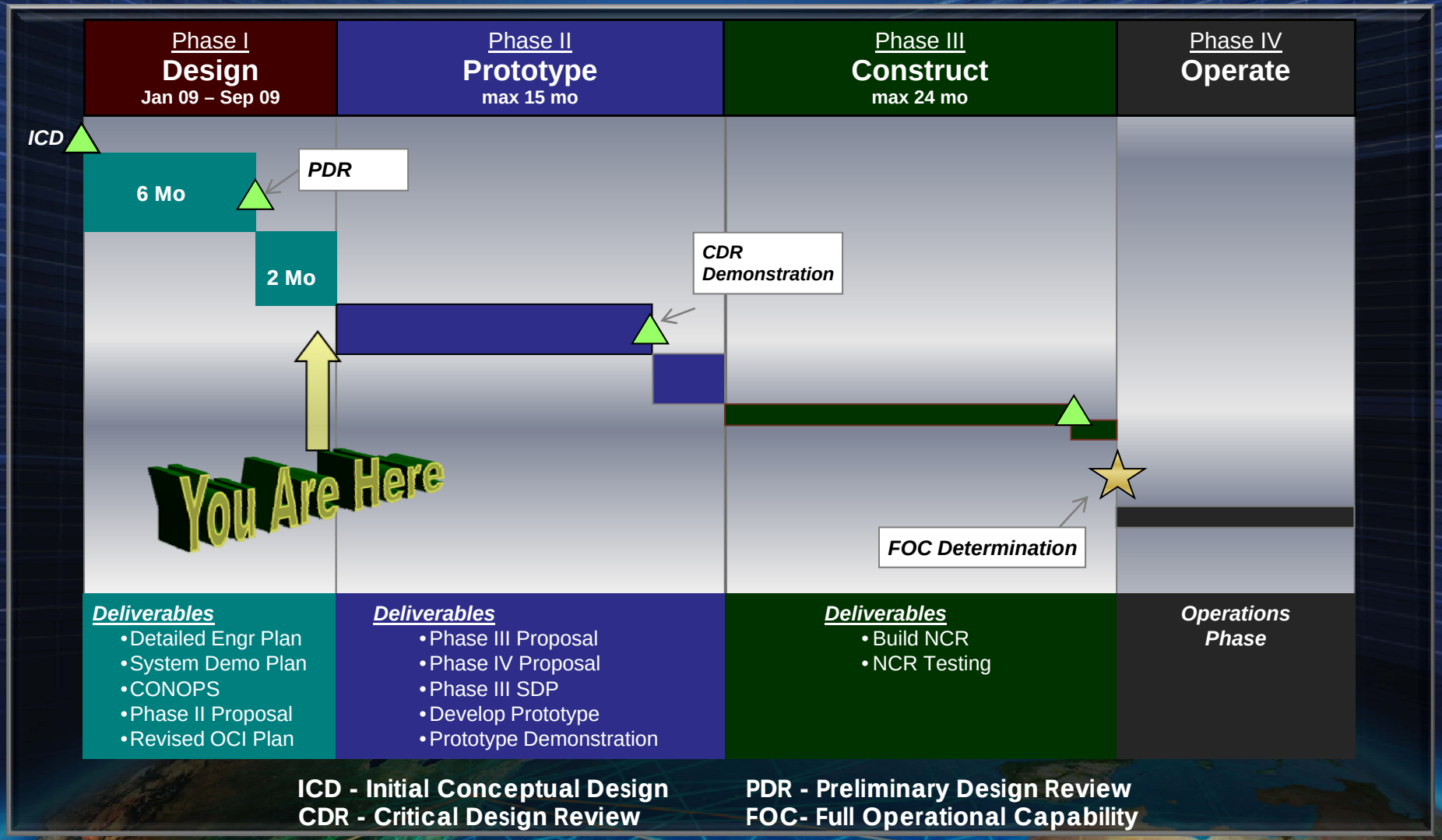
Over the ages scientific progress has been held back by the ability to make measurements at the level of the environment for which the scientific research was being done: ***Telescopes, microscopes, particle accelerators, etc.***

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 accidently into the light.

Unconstrained cyber research environment supporting the CNCI

Challenge	Today's Ranges	National Cyber Range
Security	• Single test at single security level • System protected at system-high	• Multiple simultaneous tests at different security levels • Forensic resources sanitization • A safe, instrumented environment for our national cyber security research organizations to test the security of information systems
Range Configuration & Management	• Manual configuration of machines and tests w/ scripts	• Dynamically and securely allocate thousands of heterogeneous resources across multiple simultaneous tests
Test Configuration & Management	• Manual configuration and management of tests w/ scripts	• Graphic User Interface used for configuring tests • High level language for test management and resource assignment
Usability	• Customer must bring everything to the range • Technology drives CONOPS	• Technology and configurations recipes automatically loaded • Malware repository to assist experiments • Scientific observers, attackers, & defenders provided as a service
Realism	• Tradeoff between physical (realism) and scale (emulation) • Limited wireless and MANET capability	• Large-scale (10K+) combinations of physical, virtual, and emulation • Emulate commercial and tactical wireless & control systems • Extensible for new technologies and external ranges • Chip level heterogeneous virtual machines • Integrates new protocols using or replacing the TCP/IP protocol stack
Test Time	• Constrained by real time	• Accelerate test time to reduce time for results • Decelerate test time to analyze and develop alternative results
Scientific Measurement	• Test specific raw data collection	• Qualitative and quantitative security assessment of cyber technologies • Forensic data collection, analysis, and presentation • Time synchronization across devices
Traffic Generation	• Automatons	• Traffic generators realistically emulate human behavior and frailties

Program Timeline



ICD - Initial Conceptual Design
CDR - Critical Design Review
PDR - Preliminary Design Review
FOC- Full Operational Capability

NCR Team

Providing the environment to solve the Nation's Cyber problems

How can you participate?

Government Working Groups

- Security Accreditation Working Group
- Joint Working Group

Upcoming Conference and Workshops

- Quantifying Computer Security
- Science of Cyber Testing
- CONOPS Development
- Technical Transition Test Queue

Technical Correspondence

DARPA Program Manager -- Dr. Michael VanPutte
michael.vanputte@darpa.mil

DARPA/STO
ATTN: STO: Dr Michael VanPutte
3701 North Fairfax Drive
Arlington, VA 22203-1714

Unclassified fax: (703) 248-1800

Program Website: http://www.darpa.mil/sto/ia/ncr.html