The Future of Cyber Experimentation and Testing

The U.S. NATIONAL CYBER RANGE

Michael VanPutte, Ph.D.
Program Manager

Distribution Statement “A” (Approved for Public Release, Distribution Unlimited #14014)

DISCLAIMER: The views, opinions, and/or findings contained in this article/presentation are those of the author/presenter and should not be interpreted as representing the official views or policies, either expressed or implied, of the Defense Advanced Research Projects Agency or the Department of Defense.
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.
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

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

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

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

Phase I
Design
Jan 09 – Sep 09

Phase II
Prototype
max 15 mo

Phase III
Construct
max 24 mo

Phase IV
Operate

Deliverables
- Detailed Engr Plan
- System Demo Plan
- CONOPS
- Phase II Proposal
- Revised OCI Plan

Deliverables
- Phase III Proposal
- Phase IV Proposal
- Phase III SDP
- Develop Prototype
- Prototype Demonstration

Deliverables
- Build NCR
- NCR Testing

Operations Phase

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

Providing the environment to solve the Nation’s Cyber problems
UNCLASSIFIED: Distribution Statement “A” (Approved for Public Release, Distribution Unlimited)
Providing the environment to solve the Nation’s Cyber problems
UNCLASSIFIED: Distribution Statement “A” (Approved for Public Release, Distribution Unlimited)
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