The National Cyber Range:

A National Testbed for Critical Security Research

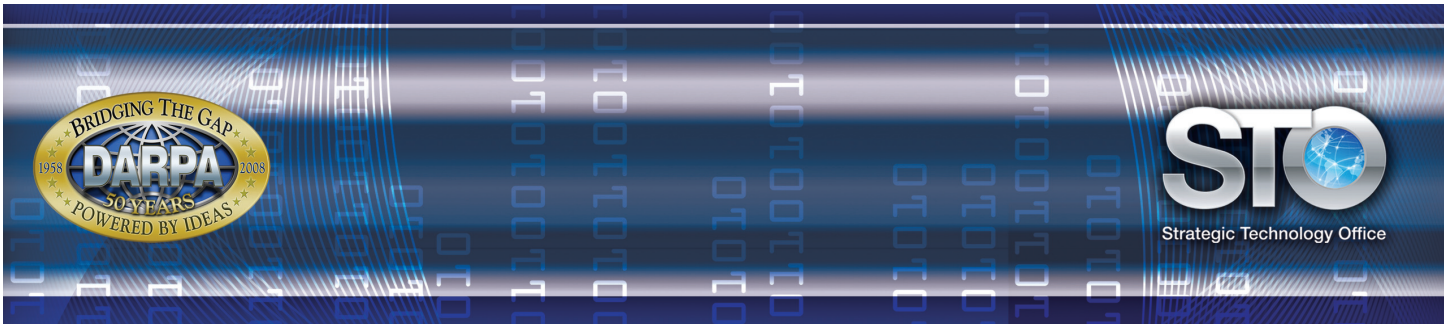
Scientific progress has frequently been constrained by a lack of adequate tools to support observation, measurement and analysis. For example, significant progress was delayed in astronomy, biology, and particle physics until advances were made in telescopes, microscopes, and particle accelerators. The Defense Advanced Research Projects Agency (DARPA) is developing the National Cyber Range (NCR) to provide realistic, quantifiable assessments of the Nation's cyber research and development technologies. The NCR will enable a revolution in national cyber capabilities and accelerate technology transition in support of the President's Comprehensive National Cyber-Security Initiative (CNCI).

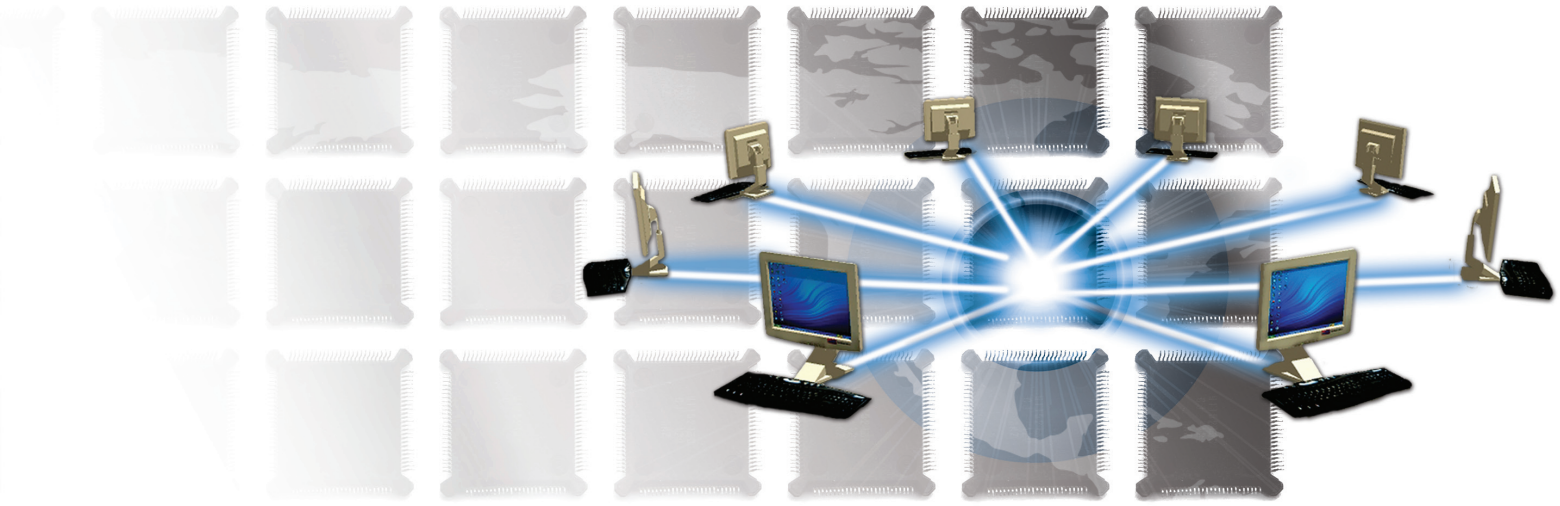
The National Cyber Range will allow classified and unclassified researchers to measure their progress in either a classified or unclassified environment, against appropriate threats, with sufficient timeliness and accuracy to allow for corrections and identify new capability needs.

DARPA is creating the National Cyber Range to protect and defend the nation's critical information systems. Leveraging DARPA's history of cutting-edge research, the NCR will revolutionize the state of the art for large-scale cyber testing. The NCR will provide fully automated range management and test management suites to test and validate leap-ahead cyber research technologies and systems, and provide vision for iterative and new research directions.

As a national resource for testing unclassified and classified cyber programs, the NCR will dynamically allocate resources to multiple, simultaneous Government and Government-sponsored tests, including on-site technical support, sophisticated offensive and defensive adversaries, and neutral observers/controllers who will evaluate cyber technologies.

(over)





Testbed Support

The NCR consists of a collection of testbeds that can conduct independent tests, or be integrated into one or more larger testbeds, according to specific testing needs. The NCR will test technologies such as host security systems, and local and wide area network (LAN and WAN) security tools and suites by integrating, replicating or simulating the technologies. The NCR will provide a large-scale Global Information Grid (GIG) infrastructure, where technologies and systems can be analyzed and tested under real world conditions in current and future environments. These testbeds include the ability to test new network protocols, satellite and radio frequency (RF) communications, and mobile tactical and maritime communications, in order to meet the needs of DoD Services and Combatant Commands, as well as other U.S. Government Agencies and Departments.

It is essential to fully understand system vulnerabilities in order to correct or mitigate them. Vulnerabilities can arise from the component to the system level, and from events such as buggy code, misconfigurations, and user actions. The NCR must be able to test all of these issues by recreating the complex interactions of real integrated systems and their human users.

The NCR will forensically collect, analyze, visualize, and present data and information from the tests. Knowledge and insights gained during testing will assist operators and developers as they refine, research, and develop operations, technologies, policies, and procedures to strengthen cyber security.

Program Status

DARPA's Strategic Technology Office issued a Broad Agency Announcement in May 2008 for Phase I of the NCR implementation that will allow selected performers to refine initial conceptual designs, develop Concepts of Operation, and produce detailed Engineering and System Demonstration Plans. Subsequent phases will support development of prototype ranges to demonstrate capabilities, and eventual full-scale NCR development and evaluation.

For more information visit http://www.darpa.mil/sto/solicitations/BAA08-43/index.html or email baa08-43@darpa.mil