

NATIONAL CYBER RANGE QUESTIONS AND ANSWERS

What is the Comprehensive National Cybersecurity Initiative (CNCI)

On January 8, 2008, President Bush issued National Security Presidential Directive 54/Homeland Security Presidential Directive 23, which formalized the “Comprehensive National Cybersecurity Initiative” and instituted a series of continuous efforts to further safeguard our federal government systems from cyber threats and attacks.

The CNCI is focused on three key areas:

- Establish a frontline defense (reducing current vulnerabilities and preventing intrusions);
- Defend against the full spectrum of threats by using intelligence and strengthening supply chain security; and
- Shape the future environment by enhancing our research, development and education as well as investing in leap-ahead technologies.

What is the National Cyber Range?

Our nation does not have a dedicated place to conduct cyber security experiments. The National Cyber Range is DARPA’s contribution to the new federal “Comprehensive National Cyber Initiative,” providing a “test bed” to produce qualitative and quantitative assessments of the security of various cyber technologies and scenarios. We will provide a revolutionary, safe, instrumented environment for our national cyber security research organizations to test the security of information systems.

What is the ‘cyber threat’?

The U.S. has been aware of and has responded to malicious cyber activity directed at the U.S. Government over the past few years. This activity is growing more sophisticated, more targeted, and more prevalent.

Cyber threats don't come in one variety. They include a very broad range of nefarious activity -- from a single individual acting as a hacker to an organized criminal group trying to steal personal or financial information to exploit for ill-gotten gain, to a hacker trying to breach a system simply in order to show that he or she can do it, to nation states engaged in cyber espionage against governments and businesses. And, finally, there is certainly the prospect of a terrorist group seeking to hijack and exploit the Internet to cause very real damage to our systems and to our country.

Malicious attacks are often used to steal information and/or disrupt, deny access to, degrade or destroy critical federal information systems. These attacks have the potential to prevent – at minimum - the efficient operations of vital government systems. Because of the interdependence of our society and our economy on information systems, a cyber attack would have cascading effects across the country and across the world.

Why can't we defend against these threats today?

This is a complex question.

First – many of the commercial systems we rely on today were designed for use in home and small businesses, and were not designed from the bottom-up to operate in hostile environments.

Second - with increased Internet connectivity, there is more access from more places, which offer an ever increasing number of malicious actors access to the Nation's interconnected information systems on which we rely at home and at work.

Third – cyber adversaries can adapt rapidly to an ever-changing environment, and are able to attack at the time and place of their choosing.

Lastly, the information on which we rely is more and more complex, interconnected, and interdependent, and increasing technological complexity increases the difficulty in securing that same technology.

What are some examples of today's actual cyber attacks?

We will not comment on actual cyber attacks in the interest of national security.

Why is it necessary to develop a 'National Cyber Range'?

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. 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 CNCI.

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 and test management suites to test and validate leap-ahead cyber research technologies and systems, and provide vision for iterative and new research directions.

What are the primary logistical and technical challenges?

Large-scale cyber testing has endured numerous technical challenges that have limited its realism and scale. Large-scale cyber testing has suffered from being a tedious, manual and demanding process. A key vision of the DARPA NCR program is to revolutionize the state of the art of test range resource and test automation execution. To facilitate this vision an automated test range resources management system will be developed to allocate and protect range resources.

Additionally, by creating an automated, interactive process to design, configure, monitor, analyze, and release tests, and a vast library of system configuration plans, or "recipes," for use on the range, researchers will be more efficient with limited resources and will be able to conduct more tests and more realistic tests.

A key challenge to testing has been the inability to stress systems in an operational environment against realistic users, who do not always ‘behave’ as we would like; this is what we would describe as a full-spectrum cyber threat. Developers often create systems with basic assumptions. When we deploy systems we discover individuals who think “outside the box” - unconstrained by the engineer’s and user’s original assumptions. The NCR will provide a full-spectrum evaluation team as a service to organizations requiring cyber testing.

Finally, there are several additional technical research thrusts. These areas are designed as high-risk, high-payoff research areas that have the potential to push the Nation’s cyber test technology base. These technologies include the ability to accelerate and decelerate test time.

Who will be doing the research and the testing?

A number of private, commercial and academic institutions and enterprises will develop the National Cyber Range. The names of the contractors are: BAE Systems; General Dynamics - Advanced Information Systems; Johns Hopkins University Applied Physics Laboratory; Lockheed Martin Corp.; Northrop Grumman - Intelligence, Surveillance and Reconnaissance Systems Division; Science Applications International Corp.; SPARTA.

What kind of experiments will be run on the NCR?

The NCR will be capable of testing that ranges from testing individual machines for security properties to large-scale enterprise tests depending on the testing organizations needs and availability of resources.

What will the NCR “look” like?

DARPA has specified overarching program objectives. The NCR contractors each have their own approach to how they plan to implement these objectives, and these divergent approaches are likely to “look different” and be proprietary to the contractor.

Where it will the NCR be located?

Each contractor team will be conducting research to develop their NCR approach in various locations. Following a number of research phases, a single contractor team will be selected to build the test bed, and that contractor, in consultation with the government, will determine a location at that time.

How long will DARPA run the range?

As with all DARPA programs, DARPA will transition the operation of the NCR at a later date to an operational partner. No decision has been made on who will operate the final range.

Will be it be available as a national asset after DARPA ends its effort?

The vision of the NCR is to create a national asset for use across the federal government to test a full spectrum of cyber programs. Priorities will be established by our transition partners.

What kind of measurements will you be making?

It is up to the organization being tested to specify the measurements needed to validate and verify their program. The NCR must be designed to meet the various needs of the community.

How will they be used to develop improved protections?

Organizations being tested will learn from the results of these tests. Observations across a full spectrum of tests on the NCR will enable researchers to make informed conclusions, as well as potentially infer new research areas from the aggregation of test observations.

How is testing done now?

Testing today is manpower-intensive, reducing the range of tests that can be conducted and increasing the costs. While automated experimental systems exist they lack the scale and capabilities needed for the NCR.

What is the timetable for activity?

During the program's initial eight-month phase, contractors will develop detailed engineering plans. At the conclusion of the initial phase, DARPA will make decisions regarding future plans, which notionally could include a second phase with a critical design review, and a third phase to develop the full-scale National Cyber Range and start conducting tests.