The National Cyber Range

About NCR

The National Cyber Range (NCR), operated by the Test Resource Management Center (TRMC), provides the ability to conduct realistic cybersecurity testing, evaluation (T&E) and training. The four key components of the NCR are: a secure facility, a unique security architecture, integrated tools for cyber testing, and a multi-disciplinary staff (Figure 1). Accredited by the Defense Intelligence Agency (DIA), the NCR provides an efficient and affordable cybersecurity testing infrastructure that can operate at levels up to Top Secret / Sensitive Compartmented Information. Using state-of-the-art network isolation capabilities, the NCR can simultaneously execute up to four independent tests at different classification levels.

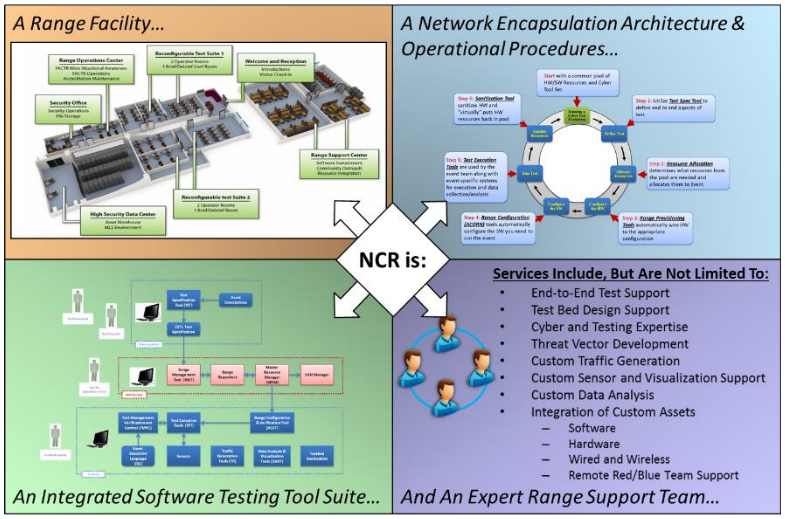

A Range Facility...
A Network Encapsulation Architecture & Operational Procedures...
NCR is:
Services Include, But Are Not Limited To:
End-to-End Test Support
Test Bed Design Support
Cyber and Testing Expertise
Threat Vector Development
Custom Traffic Generation
Custom Sensor and Visualization Support
Custom Data Analysis
Integration of Custom Assets
Software
Hardware
Wired and Wireless
Remote Red/Blue Team Support
An Integrated Software Testing Tool Suite...
And An Expert Range Support Team...

Figure 1. NCR Overview

The NCR has the ability to represent complex network topologies with sufficient realism to portray a variety of current and anticipated attack strategies. The NCR's unique security architecture and sanitization tools enable the unconstrained use of malware during test and training events. Users can conduct advanced developmental and operational tests and evaluations, and provide realistic operational training in environments that emulate their specific computing, networking, and information systems environments. The NCR's unique sanitization capability enables NCR provided test assets to be sanitized at the conclusion of an event and reused in future events at different classification levels.

The NCR enables users to assess many different aspects of cyber capabilities throughout the development and operational lifecycle (Figure 2). Events can be executed locally using secure test rooms located at the NCR or remotely via the Joint Information Operations Range (JIOR), and the Joint Mission Environment Test Capability (JMETC) in the future. Users can also integrate their program or organization unique cyber assets into an NCR environment as "black boxes" that become an integral part of the environment without the need for range security reaccreditation.

The NCR has demonstrated the ability to rapidly configure a variety of complex network topologies and scale up to 40,000 nodes. These nodes can include high-fidelity realistic representations of the public internet infrastructure including highly detailed supporting web and email servers and clients. The ability of the NCR to emulate sensitive DoD network enclaves adds a high degree of realism and value to events.

The world-class multi-disciplinary staff that operates the NCR enables DOD, Intelligence Community, and other government organizations to design and conduct effective, and cost efficient cybersecurity T&E and training events. Experts in offensive and defensive cybersecurity, testing, and software development skills can engage with users to address a wide variety of complex cybersecurity challenges.

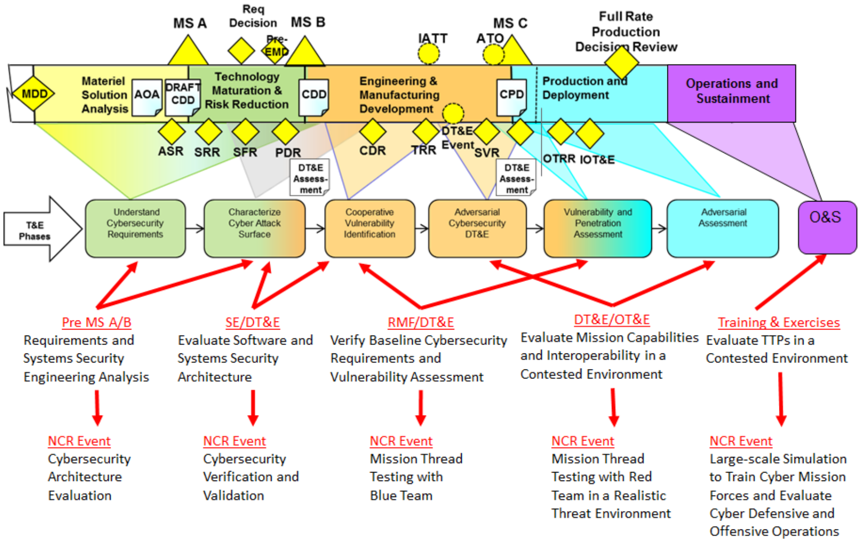

MS A
Req Decision
MS B
Pre-EMD
IATT
MS C
ATO
Full Rate Production Decision Review
MDD
Materiel Solution Analysis
AOA
DRAFT CDD
Technology Maturation & Risk Reduction
CDD
Engineering & Manufacturing Development
CPD
Production and Deployment
Operations and Sustainment
ASR
SRR
SFR
PDR
CDR
TRR
DT&E Event
SVR
OTRR
IOT&E
DT&E Assess-ment
DT&E Assess-ment
T&E Phases
Understand Cybersecurity Requirements
Characterize Cyber Attack Surface
Cooperative Vulnerability Identification
Adversarial Cybersecurity DT&E
Vulnerability and Penetration Assessment
Adversarial Assessment
O&S
Pre MS A/B
Requirements and Systems Security Engineering Analysis
SE/DT&E
Evaluate Software and Systems Security Architecture
RMF/DT&E
Verify Baseline Cybersecurity Requirements and Vulnerability Assessment
DT&E/OT&E
Evaluate Mission Capabilities and Interoperability in a Contested Environment
Training & Exercises
Evaluate TTPs in a Contested Environment
NCR Event
Cybersecurity Architecture Evaluation
NCR Event
Cybersecurity Verification and Validation
NCR Event
Mission Thread Testing with Blue Team
NCR Event
Mission Thread Testing with Red Team in a Realistic Threat Environment
NCR Event
Large-scale Simulation to Train Cyber Mission Forces and Evaluate Cyber Defensive and Offensive Operations

Figure. 2. NCR Lifecycle Support

Benefits of Using the NCR

By leveraging NCR resources, government organizations have gained valuable insights into how well their existing information technologies can meet the demands of a rapidly evolving cybersecurity landscape. With a highly scalable, secure, and extremely flexible range capability, expensive questions can be answered quickly, accurately, and safely. This can be achieved at a fraction of the cost associated with building and operating a similar customer-owned capability.

The NCR can support detailed empirical analysis such as determining whether a network security architecture will scale in the real world, determining if new cybersecurity assets will close requirement gaps, and simulating realistic network traffic using a robust suite of traffic generation tools, such as LARIAT, Breaking Point and a library of custom-developed traffic generation components.

The NCR can also help in assessing how resilient a system is to cybersecurity-attacks and faults when connected to a larger system-of-systems architecture by providing augmentations to existing operational environments. If a program wanted to evaluate the effectiveness of its cyber offensive and defensive capabilities, it could exercise and experiment with those capabilities at the NCR – with no adverse impacts to the program-owned infrastructure.

The NCR is instrumented with sensors that collect network traffic and other system resource data for reporting and after action review purposes. The sensors can capture data from local and distributed nodes.

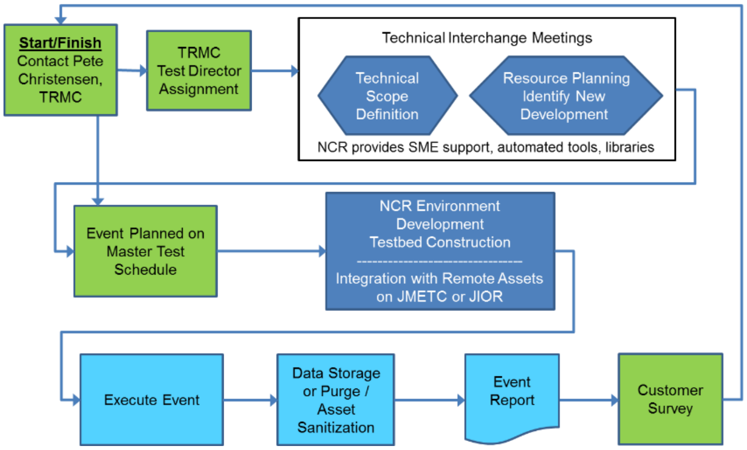
Additional Features

Customer-Driven Test Specification
NCR customers can specify how they want their testbed configured and built. Testbed profiles can be built independent of the actual test event while enabling programs to enforce their normal peer review and configuration management processes. Automated tools enable the NCR to translate and allocate customer testbed requirements to the appropriate NCR resources and build the testbed to the specification.

Wireless Testing Support
The NCR supports incorporating wireless assets into a testbed through its on-site Faraday Cage.

Supported Software
The NCR supports most major operating systems and a wide compliment of supporting infrastructure tools including routers, switches, email servers, file servers, domain controllers, web servers, firewalls, intrusion detection systems and more. Should a desired operating system, infrastructure tool or other software application not already be available, the NCR has a streamlined and efficient processes for adding additional software to a testbed.

NCR Event Workflow



Start/Finish
Contact Pete Christensen, TRMC
TRMC Test Director Assignment
Technical Interchange Meetings
Technical Scope Definition
Resource Planning Identify New Development
NCR provides SME support, automated tools, libraries
Event Planned on Master Test Schedule
NCR Environment Development Testbed Construction
Integration with Remote Assets on JMETC or JIOR
Execute Event
Data Storage or Purge / Asset Sanitization
Event Report
Customer Survey

Figure 3. NCR Event Workflow

The first step to arranging an NCR event is to contact a TRMC NCR representative (Figure 3). The NCR team will work with users to help shape the technical scope of their event, allocate resources and identify and develop any required custom integration through a series of technical interchange meetings between NCR Test Directors, technical subject matter experts, and user representatives. Once the scope of the event has been defined, the event is scheduled for range time.

Prior to execution, the NCR staff will use the test specification that is the product of the technical interchange meetings and "build out" the testbed. The build process includes the partitioning of the testbed, allocating system resources to the test, and integration and configuration of additional assets that are part of the test specification. Once the build process is complete, the testbed is ready to go "range hot" – and is prepared for the event to start.

During the event, customer-specified data can be collected for reporting purposes through NCR's suite of data sensors and visualization tools. Data that is collected during an event belongs to the customer and will be protected by the NCR in accordance with customer guidelines and will not be released and shared without first receiving the customer's approval.

Once an event has concluded, a test report is generated and all assets used during the event are sanitized—leaving no trace of an event's testbed and the data it collected behind. The testbed assets are then returned to the pool of available resources for the range.

Finally, the NCR provides customers with a feedback survey that helps the range continue to meet the challenges they face. This continuous feedback and improvement process is one component to ensuring that the NCR remains ready to support the mission.

For More Information Contact

Peter H. Christensen
Director, National Cyber Range
peter.h.christensen.civ@mail.mil
571-372-2699

4800 Mark Center Drive
Suite 07J22
Alexandria, VA 22311