Distributed testing is the linking together of various live, virtual, and constructive (LVC) sites and capabilities in order to conduct the test and evaluation (T&E) of a system or a system of systems. While distributed testing is not meant to replace live, open-air testing, it is a tool that can use actual live operational hardware in a distributed environment, in lieu of a large-scale open-air test. Conducting distributed testing provides a means for rapid integration of systems early in a program's developmental life cycle, thereby reducing the technical risk of the program. Distributed testing enhances the cross-flow of test data between T&E agencies and allows for the early integration of operational-test influence into development test. In these times of cutbacks and austere budgets, distributed testing has a proven and reliable record of saving acquisition and T&E programs time and money. However, it still is a new way of thinking for many in the acquisition and T&E communities.

In December 2005, the Department of Defense (DoD) directed the development of the Joint Mission Environment Test Capability (JMETC) Program to provide the test infrastructure necessary for conducting joint distributed test events by cost-effectively integrating LVC test resources configured to support the users' specific needs for each event. JMETC was placed under the Under Secretary of Defense for Acquisition, Technology, and Logistics, with responsibility for execution assigned to the director of the Test Resource Management Center (TRMC). In October 2006, the JMETC Program Management Office was established under the TRMC. JMETC provides the connectivity and technical support enabling testing "early and often" across the full spectrum of the acquisition life cycle, which allows for the identification of technical and operational concerns to program offices and DoD leadership. JMETC enables a near-real-time “test-fix-test” process as well as an integrated methodology of development and operational test, providing information early in a system's development process, when it is easier and cheaper to correct problems. JMETC has supported distributed testing events for all the Services, many joint programs, and even coalition events. In one recent event, JMETC supported a joint urgent operational need, providing the distributed infrastructure needed to test the integration of a classified command-and-control payload onto multiple air platforms. This program, designed to resolve the challenges of in-theater beyond-line-of-sight communications limitations, required a complex test infrastructure supporting live-fly developmental testing and an operational utility assessment. The JMETC-supported distributed test event allowed for the efficient integration of development and operational test, and enabled the off-site participation of required test assets that were not available on-site. In completing this distributed test, an urgent capability was fielded quickly to support combat forces, and the lead test organization reported that they saved $1.2 million in anticipated test costs—a success directly attributed to JMETC and distributed testing!

While JMETC has demonstrated a consistent ability to save customers time and money, a standout benefit of JMETC is the engineering-risk reduction in providing readily available, persistent connectivity with standing network-security agreements, common integration software for linking sites, and accredited test tools. JMETC’s unique total-package support allows T&E customers to minimize the technical risk associated with planning for and executing the distributed test infrastructure so that they can truly focus on their test requirements. This more efficient approach of using distributed testing directly supports significant improvements in joint combat capability by enabling the T&E community to field a better, more interoperable product quicker and at less cost!

To accomplish its mission, the JMETC program:
- maintains a core reconfigurable foundation that enables the rapid integration of LVC resources;
N has developed products that provide not only readily available connectivity over existing DoD networks, but also standard data-transport solutions, tools and utilities for planning and conducting distributed integrations, and a reuse repository; N has developed and maintains an established infrastructure with many sites and systems already connected (see Figure 1); and N provides both on-site and help-desk customer support for use of the JMETC infrastructure to integrate LVC resources.

JMETC is constantly adjusting to the changing needs and requirements of its customers. Perhaps one of the most urgent and dynamic mission areas in today’s global environment is that of cyber warfare. To be relevant in today’s cyber environment, T&E must accurately and affordably measure cyberspace effectiveness and vulnerabilities of warfighting systems and DoD information systems to verify the warfighters’ capability to achieve mission success while operating in cyberspace. The JMETC Program Office is poised to take on the additional tasking of the cyber-test mission. JMETC is already in the process of evaluating what investments and capabilities will be needed and is developing a vision for building cyber T&E infrastructure, methodology, workforce, and tools. A key part of the cyber T&E infrastructure was put in place in the fall of 2012 with the transition of the National Cyber Range (NCR) into the TRMC. Now the positions of JMETC program manager, and director of the NCR are held by the same person.

The National Cyber Range originated as a Defense Advanced Research Project Agency program focused on addressing the challenge of testing cyber technologies. Testing in a realistic environment is critical to developing confidence that mission goals will be achieved when operating in the cyber domain. Standing up realistic environments tailored to specific missions and test requirements is challenging because of the large variations in environments—operating-system versions,
application versions, network topologies, Internet protocol address configurations, router configurations, user policies, etc.—that exist across DoD, deployed bases, NIPR Net, SIPR Net, the public Internet, and a myriad of other networks comprising the cyber domain. The integrated tool suite developed for the NCR addresses these challenges, namely deploying realistic, large-scale cyber test environments tailored to a specific test requirement reliably, rapidly, and repeatedly.

Under the National Cyber Range Program, the JMETC team can now provide its customers the unique capability that includes a secure framework to rapidly emulate military and adversary networks to perform realistic cyber test, as well as cyber mission rehearsal. The NCR provides a common cyber test and training range that enables:

- rapid creation of high-fidelity virtual cyber environments—in hours, not months—that enable realistic cyber testing and training;
- repeatable results to build confidence in cyber test results;
- precise control of the test environment that enables the rapid variation of environmental conditions to quickly evaluate hundreds of scenarios;
- flexibility to replay scenarios, either as originally executed or by varying one or more parameters, to improve speed and test/training effectiveness;
- more time to test and/or train rather than expending time and resources in developing and setting up events; and
- sanitization of the resources after the event so those resources can be reused in future events.

There are four main components of the NCR: the facility and physical computing assets, the encapsulation architecture and security procedures, the automated-testing tool suite, and an experienced cyber-test team. When leveraging these four elements, the NCR provides the ability to create and manage high-fidelity test environments that support rapid and effective evaluation of advanced cyber technology, threats, and missions (see Figure 2).

The NCR facility is a secure range facility (fully accredited to handle Top Secret/Sensitive Compartmented Information) that enables multiple independent tests of differing security levels to be simultaneously executed. The facility contains two independent test suites enabling concurrent execution of tests at different security levels or

Figure 2. Four elements of the National Cyber Range (NCR). The NCR leverages a common pool of resources to create isolated test beds. The common pool of resources is made up of servers, network devices, specialty devices such as packet-capture appliances, and software including operating systems, tools, and applications. The range-management enclave manages the common resource pool and leverages the encapsulation tools to create a security boundary between test beds and a controlled interface between each test bed and the range-management enclave. The encapsulation architecture enables each test bed to be run at different security levels and then, when a test is completed, sanitizes the resources and puts them back into the common pool for reuse. Once resources are allocated and security boundaries are set up, the automation tool kit configures the allocated resources into the network topology and configures the software on the servers to represent the test architecture.
The NCR security procedures and encapsulation architecture provide a defense-in-depth approach that balances many competing factors including isolation, test-bed deployment/reclamation times, equipment cost, test performance fidelity, and accreditation risk. They are specifically designed to allow simultaneous tests to operate at different security levels/compartments while meeting ICD503 certification and accreditation requirements. They combine a system high-range management infrastructure with a multiple independent levels of security range-asset partitioning capability that can dynamically build and manage a large number of isolated test beds operating at various security levels.

- The NCR automated tool set is a unified set of integrated tools that supports the automated construction and verification of high-fidelity test beds in very short periods of time. It includes tools to specify a test, automatically construct and verify a test bed, execute a test (including test-bed reconfiguration and reconstitution), and analyze and visualize test data. The tool set provides a significant reduction in the time it takes to define, develop, and implement a cyber test, reduces the risks of configuration errors, and enables the reuse of expertise and configurations developed in support of a particular test.
- The experienced cyber-test team provides end-to-end test support from defining an effective cyber test and conducting test events to analyzing data.

The National Cyber Range has already been overwhelmingly successful at conducting distributed experiments, has been a node on the Joint Information Operations Range during events, and has demonstrated the capability to rapidly emulate the complexity of defense and commercial networks, allowing for cost-effective and timely testing and validation of cyber technologies. The JMETC Program Office is poised to take on the cyber-test mission in FY13, and is already investing in the necessary cyber infrastructure and standards for this rapidly evolving mission area. In addition to continuing to make improvements to distributed test infrastructure and support, as well as maturing the NCR capabilities for distributed T&E use, JMETC is committed to developing cyber T&E use cases, building a cyber T&E support cell, supporting cyber T&E events, and partnering with multiple other agencies and programs involved in cyber T&E. If you would like more information now, or need to query us regarding distributed testing support or the NCR, please contact:

Mr. Bernard "Chip" Ferguson  
Deputy Director, Interoperability and Cyber Test Capability, Test Resource Management Center (TRMC)  
Director, National Cyber Range  
Program Manager, Joint Mission Environment Test Capability (JMETC) Program  
Test Resource Management Center  
4800 Mark Center Drive, Suite 07J22  
Alexandria, VA 22350-2700  
Tel: (571) 372-2697  
chip.ferguson@osd.mil

MR. BERNARD “CHIP” FERGUSON is the deputy director for interoperability and cyber-test capability at the Test Resource Management Center (TRMC) and the program manager for TRMC’s Joint Mission Environment Test Capability Program. Since joining the Army in 1965, Mr. Ferguson has held leadership positions in combat units, varied level staffs, the Army’s Operational Test and Evaluation Command, and the Office of the Director, Test and Evaluation, Office of the Secretary of Defense. Upon retirement from active duty, Mr. Ferguson became a division manager and operations manager with Science Applications International Corporation supporting test and evaluation in DoD. With his vast experience in distributed testing and evaluation, Mr. Ferguson was selected for his current position in 2006.