

# Report Documentation Page

Form Approved  
OMB No. 0704-0188

Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

1. REPORT DATE <b>OCT 2005</b>		2. REPORT TYPE		3. DATES COVERED <b>00-00-2005 to 00-00-2005</b>	
4. TITLE AND SUBTITLE <b>Wanted: A New Test Approach for Military Net-Centric Operations</b>				5a. CONTRACT NUMBER	
				5b. GRANT NUMBER	
				5c. PROGRAM ELEMENT NUMBER	
6. AUTHOR(S)				5d. PROJECT NUMBER	
				5e. TASK NUMBER	
				5f. WORK UNIT NUMBER	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) <b>Air Force Materiel Command, Electronic Systems Center, Hanscom AFB, MA, 01731</b>				8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)				10. SPONSOR/MONITOR'S ACRONYM(S)	
				11. SPONSOR/MONITOR'S REPORT NUMBER(S)	
12. DISTRIBUTION/AVAILABILITY STATEMENT <b>Approved for public release; distribution unlimited</b>					
13. SUPPLEMENTARY NOTES					
14. ABSTRACT					
15. SUBJECT TERMS					
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT <b>unclassified</b>	b. ABSTRACT <b>unclassified</b>	c. THIS PAGE <b>unclassified</b>			

## Wanted: A New Test Approach for Military Net-Centric Operations

David J. Carstairs

Electronic Systems Center, Air Force Materiel Command,  
U.S. Air Force, Hanscom Air Force Base, Bedford, Massachusetts

**J**oint Vision 2020, the plan for military superiority by the Department of Defense (DoD), calls for the U.S. Armed Forces to be faster, more lethal and more precise than they are today.

Achieving a decisive military advantage is the idea behind net-centric operations, which enable U.S. military forces to share all the relevant information about a situation. Achieving net-centric operations will allow U.S. forces to operate with greater initiative and situational awareness, allowing increased speed of command.

The idea is that everybody will receive all the information they need, when they need it. Any level of net-centric operations depends on a supporting environment called the Global Information Grid (GIG). The GIG provides the end-to-end set of capabilities, processes and personnel to manage and provide information on demand to warfighters, policy makers and supporting personnel. But providing information is only part of achieving military superiority. We also need rapid, agile test and evaluation (T&E) of command and control (C<sup>2</sup>) enterprise capabilities to ensure system interoperability and operational security.

We are now fighting an enemy that changes tactics practically daily. We are fighting wars in Afghanistan and Iraq while keeping our eye on hotspots such as Syria, Korea and Iran. Yet, while hostilities throughout the world have increased during the past several years, U.S. force structure has been reduced. Military personnel are being reduced in number through personnel drawdown; facilities are being lost through Base Realignment and Closure activities; and weapon programs are experiencing budget cuts. We do not have the luxury of taking six months to react to new military crises.

### Speed of command

In the former Cold War environment, combat capability was increased by adding more platforms, such as

the U.S. Air Force's F-15 Eagle, Airborne Warning and Control Systems (AWACS) and others. But to offset the trend of using fewer platforms in today's world, DoD is using net-centric operations to generate battlespace awareness and to increase its speed of command. Improving speed of command puts decision makers more in sync with shooters and transforms warfare from discretely escalating steps to a continuous process.

Warfighters will be able to create new offensive and defensive capabilities by quickly reconfiguring their systems to accept and transmit data from sensors, as well as information about threats and targets. However, current T&E processes could be an impediment if net-centric capabilities need to be fielded faster than our adversaries apply new threat technologies. It is difficult to predict what new capabilities will be required, so our T&E infrastructure must be flexible enough to accommodate rapid evolution for a timely response.

One of the major problems facing DoD is providing sufficient interoperability throughout the C<sup>2</sup> enterprise. If we consider the generic enterprise as three increasingly complex levels, we can see how T&E becomes increasingly problematic. At the lowest level, optimizing individual programs or systems is straightforward. The second level increases T&E complexity because systems are combined into a system-of-systems in which interoperability is critical. The third level, the enterprise, is the most complex and the level at which joint and coalition operations are conducted. Current T&E concepts do not scale to this level because they do not address the many possible interdependencies among the complex systems in a C<sup>2</sup> enterprise.

Another problem in testing complex systems involves addressing all relevant mission threads. A mission thread is an end-to-end, ordered sequence of activities that provide a capability (for example, to attack and



*David J. Carstairs*

destroy a target). To completely test a capability would involve testing all of its threads. Any new enterprise T&E effort should focus on evaluating overall mission capabilities and using mission threads for sample testing. In other words, if net-centric operations provides a capability, and that capability can reconfigure processes for many mission threads, we want to evaluate the envelope of enterprise capability, not just a set of constituent threads.

### New paradigm is needed

As DoD continues developing its net-centric operational capabilities, a new T&E paradigm must be developed to keep pace with DoD's changing capabilities and the ability of our adversaries to throw new threats at us (see Figure 1). Recognizing that testing all C<sup>2</sup> mission thread possibilities is impossible, the paradigm then has two parts. First is a network infrastructure for T&E that is always in place. This avoids the expense of building a network for every new capability and mission and then tearing it down after testing. Second is the ability to quickly test new technologies and capabilities.

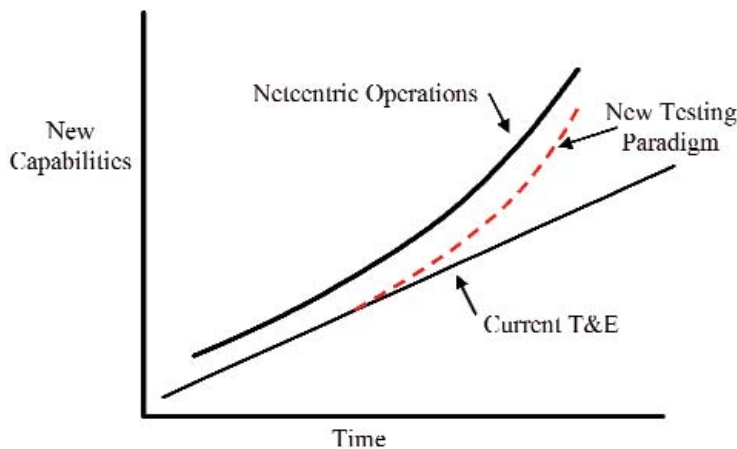


Figure 1. Network operations are changing so quickly that current T&E processes cannot keep pace. A new testing paradigm (dashed red line) needs to be developed to close the gap.

One solution is to create an infrastructure independent of the GIG. For now, call it a Collaborative Test Environment, or CTE. "Collaborative" is the operative word, both in planning a CTE and in using it. By necessity, a CTE will be a distributed environment—a federation of new and existing facilities from commercial, military and not-for-profit organizations. Every military service should own a piece of it. Facilities run by not-for-profit companies such as the

MITRE Corporation and the Massachusetts Institute of Technology's Lincoln Laboratory could also participate.

### Linking facilities

Almost every organization that might be interested has one or more of the pieces that could contribute to a CTE: laboratories, test facilities, simulators and so forth. For example, the military services have facilities such as the:

- Joint Systems Integrated C<sup>2</sup> Center
- Air Force C<sup>2</sup> Enterprise Integration Facility (CEIF)
- Air Force Combined Air Operations Center-Experimental (CAOC-X)
- Joint Interoperability Test Command (JITC) Defense Information Testbed
- Army Digital Integrated Laboratory (DIL)
- Naval Center for Tactical Systems Interoperability (NCTSI)
- Contractor facilities

*(Note: These facilities have not endorsed the strawman CTE concept, but are mentioned as examples of a potential CTE infrastructure.)*

### Save time, reduce GIG vulnerabilities

A CTE would allow DoD and U.S. allies and coalition partners to simulate parts of the network that may not yet exist, facilitating modeling evaluation of new capabilities in ways that have not been possible before. Such capability modeling/simulation would evolve to reveal potential responses to postulated and real threats. Those modeled capabilities and observed responses could then be verified in a CTE network environment to determine their operational benefits and to support rapid deployment. If a CTE could

tap into the evolving C<sup>2</sup> enterprise network, it would eliminate the impractical need for replication of a large operational network time after time.

To develop the best net-centric operations capabilities, a range of CTE users should participate. As the Joint Distributed Engineering Plant (JDEP) has proposed, a collaboration of warfighters, testers and developers is critical. However, a CTE must be devoted to the evaluation of net-centric operations in

a realistic C<sup>2</sup> enterprise. Early involvement in development activities by the operators and testers will make them more familiar with new T&E concepts for the C<sup>2</sup> enterprise, making testing more efficient. The operators and testers can then help define and refine test procedures to make them more effective in achieving test objectives. Early collaboration also can establish confidence in test results and address difficult-to-test situations, especially those that require long durations in realistic operational environments. Early involvement would also facilitate designs of experiments to test the boundaries of the capability envelope, providing greater confidence in the robustness of new capabilities.

### Vulnerability testing

A CTE would be useful in testing applications vulnerabilities, as well as their interoperability, so that the GIG is not disrupted and remains secure. An internal team of “good guy” hackers could poke at a CTE to discover any vulnerability. Security control would be a DoD responsibility. The goal of making data available to everyone anytime makes testing communications extremely important, both for vulnerability and operations. Currently, DoD communications connectivity exhibits tremendous heterogeneity with a wide variety of bandwidths, costs, security levels and contention. For example, an F-15 may not have the ability to receive data within the same bandwidth as the Army ground station that sends the data.

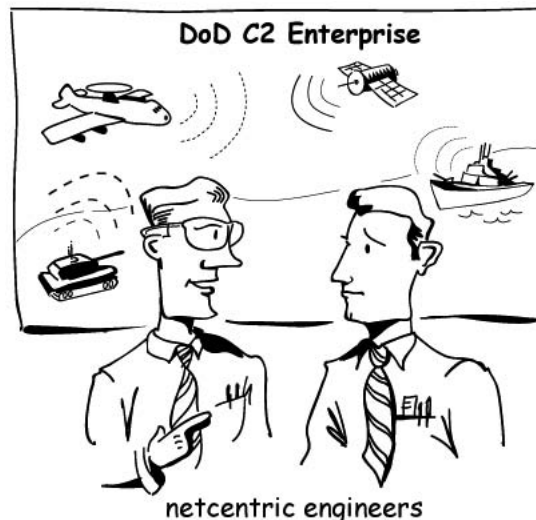
From a C<sup>2</sup> enterprise perspective, the key is to begin pulling together disparate systems with vested interests in collaborative frameworks to address operational issues with minimal recurring communications infrastructure costs. Critical to this initiative is the ability to understand the limitations inherent in sending data from one platform to another or from one network architecture to another.

### Physical infrastructure

Although connecting facilities takes time and funding (for example, to lease communications lines), these issues are typically not show-stoppers. Often, communications “pipes” that have been sized for simultaneous-use or stressing applications have underutilized capacity that could be shared by a CTE, resulting in cost savings. More flexible connectivity arrangements with constant low-level operational use is highly desirable for C<sup>2</sup> enterprise applications and can accommodate brief on-demand bandwidth-spiking. Flexibility and adaptability are the keys.

### Conclusion

A CTE would address an existing void in net-centric T&E capabilities for DoD’s C<sup>2</sup> enterprise. A CTE could provide rapid T&E of new C<sup>2</sup> technologies and changing missions for DoD. With a readily available infrastructure, existing test networks could be flexibly linked together as needed, thus saving valuable resources. Given these challenges and the promise of enhancing our warfighting capability, is it possible that stakeholder organizations can collaboratively develop a new T&E paradigm for the C<sup>2</sup> enterprise? □



"We've got a great new capability, but we've got to wait 6 months for T & E to check it out on the enterprise."

*DAVID J. CARSTAIRS, a member of the Senior Executive Service, is director, Network Centric Operations/Integration Wing, Electronic Systems Center, Air Force Materiel Command, Hanscom Air Force Base (AFB), Massachusetts. As director, he is responsible for a*

*portfolio valued at more than \$20 billion in three critical mission groups: Global Information Grid Systems, Enterprise Integration and Global Air Traffic Systems. Prior to his current assignment, he was director of Defense Information Infrastructure-Air Force Systems Program Office, Hanscom AFB. Previously, he was the system program director for the Strategic and Nuclear Deterrence Command and Control Systems Program Office, Peterson AFB, Colorado. Carstairs has held management positions in various Air Force communications programs and in acquisition support and development.*