Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
JUL 2007		**00-00-2007 to 00-00-2007**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Sharing Information Today: Net-Centric Operations in Stability, Reconstruction, and Disaster Response	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) **Assistant Secretary of Defense (Networks and Information Integration),6000 Defense Pentagon,Washington,DC,20301**	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
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES
CROSSTALK The Journal of Defense Software Engineering, July 2007

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. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**Same as Report (SAR)**	**2**	

Sharing Information Today: Net-Centric Operations in Stability, Reconstruction, and Disaster Response

Dr. Linton Wells II
Principal Deputy Assistant Secretary of Defense (Networks and Information Integration)

As the Department of Defense (DoD) continues its information age transformation to net-centric operations, we must consider the full array of the DoD's activities. The level of interaction with partners outside the boundaries of DoD networks has increased tremendously over the past few years. In particular, it is crucial to support Stability, Security, Transition and Reconstruction (SSTR) operations, Humanitarian Assistance and Disaster Relief (HADR), and Building Partnership Capacity (BPC) among potential coalition members. The social, political, and economic goals for which United States and coalition forces are committed can only be achieved through effective interaction with these non-traditional partners in largely unclassified environments.

Net-centric operations are key elements of the DoD's information age transformation. Much has been written about net-centric approaches in major combat operations. However, the DoD also must be able to support SSTR operations, HADR, and BPC among potential coalition members. Net-centric principles must extend to these environments as well.

Thus, it is necessary to communicate, collaborate, engage, and – in some cases – translate with civil-military partners outside the boundaries of DoD networks in what often are called *complex operations*. These capabilities are not nice-to-have adjuncts to other military requirements. In fact, the social, political, and economical goals for which United States and coalition forces are committed *cannot* be achieved without the ability to interact effectively with these non-traditional partners in largely unclassified environments. Such collaborative efforts need to work with austere communications that function where power is unreliable. These capabilities are urgently needed now in Iraq and Afghanistan, and they will be needed elsewhere in the future.

As has often been said, there is no interoperability without operability. Real-world experiences – from the Balkans to Iraq and from the tsunami relief to Katrina – have shown that operations repeatedly have been impeded by a lack of *communications, lift,* and *power*.

Communications

Networks provide a means to share information, develop shared situational awareness, and self-synchronize actions in accordance with command intent to accomplish its mission more effectively. But the sensors to gather data, and the ability to share information, are not techie-geek adjuncts to major muscle movements such as the delivery of food, water, and shelter. *They are critical enablers of everything else that happens.* Such capabilities often are called *hastily formed networks* and they are essential to restoring basic voice and data services, both in disaster and stability environments. The network environment during the initial phases of a disaster response often is chaotic. Organizations may arrive with their own networks and promptly activate systems without coordinating with other participants. Radio frequency management is seldom done well. As a result, Information and Communications Technology (ICT) leaders in disaster areas must coordinate actions prior to activating their networks to minimize these types of problems. More generally, technical solutions must provide the flexibility to add unanticipated users, connect with non-traditional partners, scale to meet demands for bandwidth, and support the users with intermittent connectivity who always are involved in emergencies.

> *"Trust is essential for relationships to be established, on or offline, and for actions to be taken in stressed environments."*

Lift

Networks and their supporting equipment almost always will have to be moved into crisis locations, either to augment damaged systems or add new capabilities. But, too often, they are not given adequate priority in lift manifests to get there soon enough to enable the other actions that depend on them. Such capabilities need to be put on the first few lifts during an operation and not be relegated to follow-on echelons.

Power

Stable, reliable electrical power is essential for effective information sharing, but almost never was available in HADR environments and rarely in SSTR. In such situations, power solutions ideally would not depend on gasoline or diesel fuel, which complicate the already significant logistic problems in austere environments. Several efforts are beginning to produce rapidly deployable, sustainable power systems that can use multiple energy sources (wind, solar, biofuel, etc.), and these should be incorporated into exercises and contingency plans.

Social Networking

Technology is an important component of information sharing, but by no means the only one. Social networking is a key enabling function in fostering effective responses to complex emergencies. Trust is essential for relationships to be established, on or offline, and for actions to be taken in stressed environments. Such trust is not built overnight. It needs to be built on shared experiences and reinforced with credible identification management. The establishment of relationships with anticipated partners, well before a contingency, is critical to the success of future operations.

Data Strategy

A core tenet of net-centric operations is the underlying data strategy. This calls for data to be visible, accessible, and understandable, even for unanticipated users. The approach decouples data and applications, enabling much more flexible responses, but it also requires that data from diverse sources be tagged appropri-

ately. This can be a particular challenge when dealing with a wide range of partners. Moreover, merely creating information is not enough. This goal is to support improved decision-making and to turn decisions into actions as quickly as possible. This often involves innovation in the field.

Entrepreneurial Adaptation

The pace of technological change is breathtaking, and government systems, however well resourced, typically developmentally lag in the private sector. Moreover, planned linkages and interactions will almost certainly be overtaken by events in crises. Therefore, a critical component of an effective response is to be able to adapt existing capabilities in cooperative, entrepreneurial ways on the fly.

By taking these lessons into account, the DoD is working on five parallel fronts to extend net-centric operations to SSTR, HADR, and BPC environments:

1. Developing *capabilities* to gather situational awareness and to share it by communicating, collaborating, translating, and engaging beyond the boundaries of the *.mil* domain with non-traditional, civil-military partners in a wide variety of situations.
2. Cultivating diverse *social networks* and having them ready both to deploy quickly and to be received as trusted partners by anticipated and unanticipated partners on the scene. The DoD and its civil-military partners need to be able to assemble and share lists of available practitioners and their skill sets in trusted electronic environments.
3. Incorporating best practices *to change concepts of operations; doctrine; and tactics, techniques, and procedures*, so that appropriate action can be taken by forces on the scene without having to constantly refer issues back to higher authority.
4. Implementing *modest legal changes* that allow ICT to be used more broadly in reconstruction and repair and allow for capabilities to be left behind after the end of an operation.
5. Providing *some funding* (not much, but quickly available) to deploy these capabilities with trained personnel early enough to let them act as the critical enablers of other activities.

These approaches can transform our information sharing capabilities and greatly improve the DoD's capabilities in the critical areas of SSTR, HADR, and BPC. Establishing resilient networks and power grids in affected areas must be planned for and executed early to enable information sharing, enhance the resiliency of the local populace, and accelerate an effective response.◆

About the Author

Linton Wells II, Ph.D., serves as the Principal Deputy Assistant Secretary of Defense (ASD) (Networks and Information Integration [NII]) and was recently selected to serve as the Chair of Force Transformation and Distinguished Research Professor at the National Defense University. Prior to this, he served in the Office of the Under Secretary of Defense. Wells has more than 26 years in the U.S. Navy and has served in a variety of surface ships, including command of a destroyer squadron and guided missile destroyer. He has a bachelor's degree in physics and oceanography from the U.S. Naval Academy and a master's degree in engineering and a doctorate in international relations from The Johns Hopkins University. Wells is also a graduate of the Japanese National Institute for Defense Studies in Tokyo and was the first U.S. naval officer to attend.

SES
Principal Deputy ASD/NII
6000 Defense Pentagon
Washington, D.C. 20301
Phone: (703) 614-7323
E-mail: linton.wells@osd.mil

Web Sites

The United States Department of Defense Chief Information Officer

www.defenselink.mil/cio-nii/

The Department of Defense Chief Information Officer (DoD CIO) Web site is the homepage of the DoD CIO, offering links to legislation, policy, and communities of interest resources, as well as links to publications and articles produced by the DoD CIO. The DoD Information Strategic Plan can be found at <www.dod.mil/cio-nii/docs/DoD_IA_Strategic_Plan.pdf>. The DoD is implementing an ongoing strategic management process to enable the information assurance (IA) community to implement and manage strategic decisions, respond dynamically to changing conditions, and evolve the strategy as the situation dictates. Their ability to successfully achieve the goals in this plan requires the continued commitment and mandate from senior leadership and the cooperative support of all members of the IA community. The IA strategic plan is a living document that will continue to be reviewed for the DoD's vision, goals and objectives for relevancy, currency, and applicability to keep pace with the changing environment and address significant challenges they face.

Defense Information Systems Agency

www.disa.mil

The Defense Information Systems Agency is a combat support agency responsible for planning, engineering, acquiring, fielding, and supporting global net-centric solutions to serve the needs of the President, Vice President, the Secretary of Defense, and other DoD components, under all conditions of peace and war. They are the provider of global net-centric solutions for the nation's warfighters and all those who support them in the defense of the nation.

The Association for Enterprise Integration

www.afei.org

The Association for Enterprise Integration (AFEI) is the leading industry group providing a framework for collaboration between government and industry. The DoD CIO has turned to AFEI to be its conduit for policy and strategy input from industry through jointly chartered working groups. Scheduled events, the resource library, and news can all be accessed without membership on the Web site.