FOUNDATIONS FOR U.S.-COALITION PARTNER OPERATIONS IN A NETWORK-ENABLED ENVIRONMENT: LESSONS LEARNED

John W. Smith, Brigadier General, U.S. Army (Retired)
Martin R. Stytz, Ph.D.
Gregory N. Larsen, Ph.D.

Institute for Defense Analyses
4850 Mark Center Drive
Alexandria, Virginia 22311-1882

jsmith@ida.org (703) 578-2719
mstytz@ida.org (703) 845-6679
glarsen@ida.org (703) 845-6661

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
JUN 2005		**00-00-2005 to 00-00-2005**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Foundation for U.S.-Coalition Partner Operations in a Network-Enabled Environment: Lessons Learned	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) **Institute for Defense Analyses,4850 Mark Center Drive,Alexandria,VA,22311-1882**	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
The original document contains color images.

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**		**7**	

FOUNDATIONS FOR U.S.-COALITION PARTNER OPERATIONS IN A NETWORK-ENABLED ENVIRONMENT: LESSONS LEARNED

John W. Smith, BG, USA (Ret.)
Institute for Defense Analyses
Alexandria, VA
(703) 578-2719
jsmith@ida.org

Martin R. Stytz, Ph.D.
Institute for Defense Analyses
Alexandria, VA
(407) 497-4407
(703) 338-2997
mstytz@ida.org , mstytz@att.net

Gregory N. Larsen, Ph.D.
Institute for Defense Analyses
Alexandria, VA
(703) 845-6661
glarsen@ida.org

ABSTRACT

The trend in U.S. operations suggests an increased level of operations with a greater variety of nations as coalition partners in the future than during the Cold War. The trend also suggests that the identity and mix of those partners will continue to be defined shortly before activity commences and be defined substantially by the nature of the situation. Because of our history of involvement with a small number of "traditional" partners and allies, we tend to approach operations with new partners on a case-by-case, unique basis. We argue that DOD would be well-served if it adopted a modular approach to defining the "how-to" of coalition operations. Such an approach would necessitate the systematic exploration of each key issue that can critically influence operational results. Such a research approach would necessarily be far-reaching, evolutionary, collaborative, and require a long-term commitment.

The thesis for our research is that assessment of the combined U.S.-coalition partner force performance at forward echelons can be used to gauge the overall effectiveness of individual programs and initiatives that address culture, technology standards, organization and doctrine, and policy and law issues pursued to improve network-centric operations with coalition partners. Because operational performance is the final judge of military effectiveness, we advocate protracted, objective experimentation that will serve as the catalyst for progress in addressing culture, technology standards, organization and doctrine, and policy and law issues.

We report on two events we conducted that serve as the foundation and intellectual support for our recommended experimental approach to resolve network-related operational issues that impede successful U.S.-coalition partner operations. The events were conducted in two different venues, one a U.S.-only workshop and one a U.S.-coalition partner wargame. Each event concentrated on the issue of coalition fires—planning, but especially execution of cross-nation fire support in time-constrained, cluttered operational settings. This paper describes what we did and why—our goals, objectives, event design—as well as what we learned from the vantage points of policy, technology, and operations regarding coalition network-centric operations. The lessons learned from the events strongly suggest the need for a robust, aggressive program of experimentation coupled with technology, doctrine, organization, law and policy development undertaken to address the issues surfaced by the experiments. In the main though, the events point to a need to concentrate on the complete array of factors that can be expected to influence performance and execution in network-enabled forces if future U.S.-coalition partner operations are to achieve the high expectations mandated by DOD's transformation guidance.

1. INTRODUCTION*

As the U.S. continues to transform its national security posture to deal with the adversaries and operational realities of the 21st century, a core element of its transformation strategy is to embrace experimentation that includes the "[i]ntegration of forward deployed, CONUS based, and coalition forces into the overall Joint operation, enabling the near-simultaneous synergistic employment and deployment of air, land, sea and space warfighting capabilities." [Apr 2003 OSD Transformation Planning Guidance] Because transformed U.S. military forces are assumed to operate in the future in a network-enabled environment, it is a reasonable assumption that the goal of U.S.-coalition partner operations is an integrated, distributed force capable of coherent operations across the multi-nation battlespace. The difficult question U.S. military forces must address is defining the spectrum of issues to be addressed in order to achieve this goal. To illustrate the magnitude of the task before us, even in a U.S.-only operation there are many, key issues that remain to be resolved; in a coalition context, additional issues must be tackled and the issues that appear hard in a U.S.-only context achieve a larger magnitude of difficulty. We believe that the challenges of coalition operations will be particularly acute where differences in culture, technology standards, organization and doctrine, and

* The views expressed in this article are those of the authors and do not reflect the official policy or position of the Department of Defense or the US Government.

policy and law combine to pose persistent impediments to U.S.-coalition partner combined force performance. If coalition partner forces are to operate as interdependent forces, which we argue should be the case in a network-enabled operating environment, then a number of unique but critical factors must be addressed. These factors include seamless information sharing, policies that promote rapid intra-coalition information exchange, and concepts and procedures that can reliably guide operations, thereby permitting the promise of network-centric warfare to be fully exploited and leveraged.

The transition to network centric warfare brings with it great promise for the effectiveness of future military operations. This promise arises from the capability for network centric warfare to empower individuals at all levels with unprecedented amounts of relevant information and thereby lift the "fog of war." By achieving the promise, commanders will be able to effectively and efficiently employ their resources to achieve objectives and individuals can exploit information in real-time to increase their effectiveness in mission accomplishment and to capitalize upon transient opportunities in the battlespace. However, a central, but generally unspoken, tenet of network centric warfare is that the information received is actionable; i.e., that the information is timely and correct.

At this time, research in human factors and human behavior indicate that simply transferring information between coalition partners may not be sufficient to insure effective coalition operation, and furthermore that within a coalition operation this effective interoperation may be difficult to achieve. However, we can only speculate about the difficulties inherent in coalition network-centric operations because the experiments and exercises needed in order to elicit information about the specific difficulties that will be encountered when conducting operations with a variety of different coalition partners have not been performed. The lack of accurate data about both the difficulties to be expected and successful strategies for mitigating these difficulties raises the risks inherent in conducting coalition network-centric operations and needlessly complicates an already complex undertaking. While the problems facing us in the conduct of coalition network-centric operations are daunting, we believe that they can be successfully addressed via carefully crafted, broad-ranging experiments. These experiments will not only serve to identify issues that arise when conducting coalition network-centric operations but will also help to identify solutions or at least strategies that serve to mitigate the issues that arise for different coalition partners.

This paper reports on two events that the Institute for Defense Analyses conducted to explore the prerequisites for effective future U.S.-coalition partner (CP) military operations. Motivating these research efforts in general were DoD's transformation as well as specific programs, such as the U.S. Army's Future Combat Systems, each of which is attempting to develop and field force capabilities that satisfy DoD's stated attributes for future U.S. transformed forces.

To understand how DoD views success in the network-centric arena, one need look no further than the Department's transformation guidance, in which it explained that a core element of the transformation strategy is to embrace experimentation that includes the "[i]ntegration of forward deployed, CONUS based, and coalition forces into the overall Joint operation, enabling the near-simultaneous synergistic employment and deployment of air, land, sea and space warfighting capabilities." A key reason for this approach is further explained by the Secretary of Defense's desired outcome for transformation: "fundamentally joint, network-centric, distributed forces capable of rapid decision superiority, and massed effects across the battlespace." [1]

2. INVESTIGATION AND EXPERIMENTATION APPROACH

To investigate how to improve U.S.-CP operations, we conducted two events: 1) a U.S.-only workshop, attended by Defense, joint, and Service representatives from the operational, policy, and technology arenas; and 2) a U.S.-Singapore table-top wargame.

Although the events differed in execution, both used the same experimental approach. Two questions drove event design:

1. What is the general framework within which we should explore successful U.S. - CP operations?
2. How should we structure the events specifically to get meaningful results?

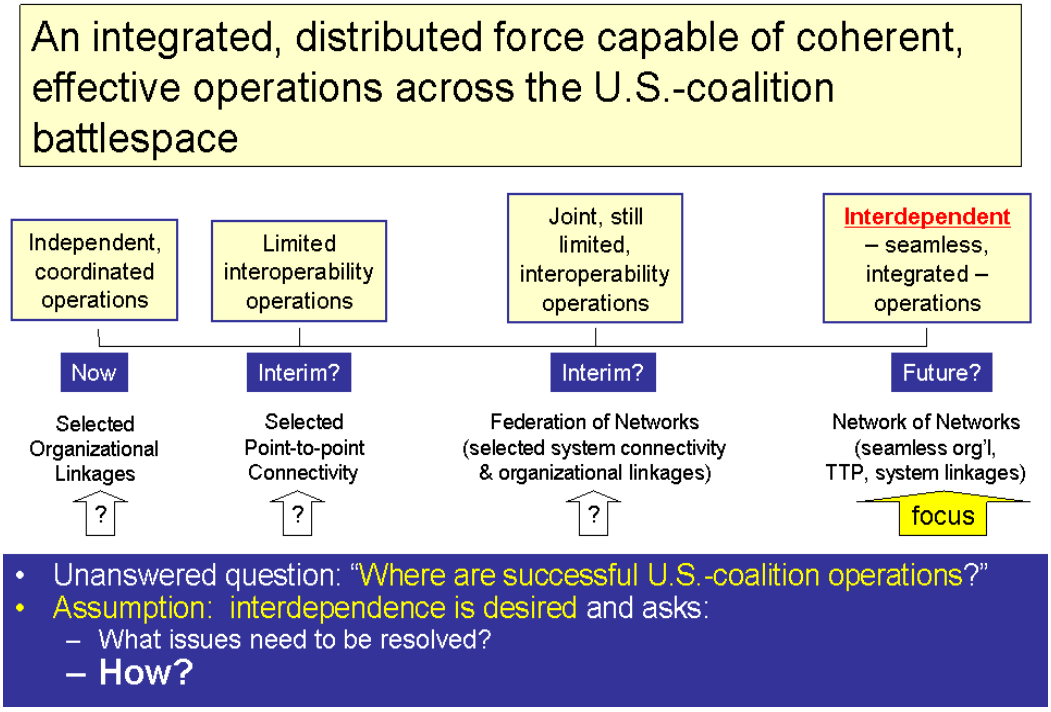

Figure 1. Assumed goal of U.S.-coalition partner operations

Figure 1 illustrates how we addressed the first question. Our approach acknowledges that there are increments of capability that might be argued by different audiences as capability that can be regarded as representative of that intended by U.S. force transformation. The figure illustrates essentially what is today's capability on the left-hand side of the figure—independent, but coordinated operations that are frequently characterized by an exchange of national liaison officers. The figure allows for interim states of various levels of interoperability, but asserts that interdependence, not interoperability, is the assumed, desired end-state for transformation. This begs the question, "What's the difference?" In essence, we view interoperability as addressing the "connectivity" issue—one system or family of systems physically able to connect with another and able to exchange data. Interoperability is a necessary, but not a sufficient, condition for interdependence. Interdependence, on the other hand, is the "condition where an organization or entity must rely on an external means (materiel capability or organizational or human behavior) to accomplish its mission." Interdependence, not interoperability, is the essence of network-centric warfare and therefore is a non-negotiable mandate if the intent of U.S. force transformation, as described earlier, is to be fulfilled.[2]

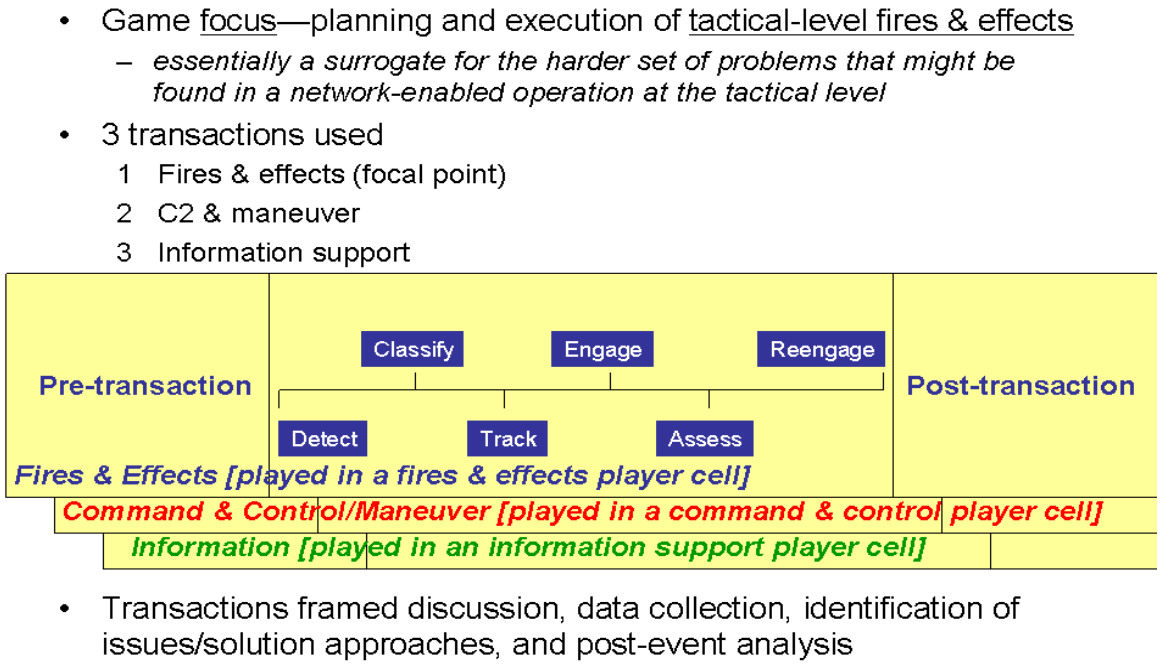

Figure 2. Wargame foundation: the battlespace "transaction"

The second question is addressed in Figure 2. It illustrates what we called the battlespace "transaction"—a structured framework to understand system, personal, and organizational exchanges and interactions in each important functional area for a given mission and scenario context. Because fires and effects, especially at forward tactical echelons, represent a hard set of operational problems that exist today and can be expected in the future, we employed a tactical-level fires-driven scenario in both events. Specifically, we placed a U.S. Army brigade adjacent to a coalition partner brigade. We incorporated activity in both built-up urban and open terrain. We employed "dilemmas" as the vehicle to present specifically constructed tactical fires situations that embodied hard issues that the players were directed to "solve." For instance, one dilemma required players to coordinate and execute a boundary change between the two brigades due to a change in the operational situation. Another dilemma required players to plan and execute cross-nation, cross-echelon fires and effects. As part of their output, players were directed to present end-to-end solutions, characterizing policy, operational, and technology solutions that were, in their view, needed to resolve the dilemma—in the framework of network-enabled, integrated, peer-to-peer operations at the forward decision-maker level. Stated another way, the game construct directed players away from reliance on today's organizationally-dependent hierarchical procedures.

3. OUTCOMES

Both events yielded similar findings and observations that suggest the adoption of several strategic directions if DoD's transformation guidance is to be realized.

Figure 3 identifies the nature of the challenge—not just for the U.S. transformation effort, but for those whom we regard as potential coalition partners. Both the U.S.-only and the U.S.-Singapore wargame found that interdependence is much more than a technology-only set of challenges. There must be concerted effort to explicitly integrate both technology and user views about how to minimize man-machine impedance across each of the performance domains that has the potential to influence the efficiency, effectiveness, and timeliness of future U.S.-CP operations. There must be an explicit effort to integrate technology and the user on the U.S. side. There must be an explicit effort to tackle the same set of challenges on the coalition side of the equation. And as difficult as both of those sets of challenges may prove to be, it is essential to grasp that the integration of user and technology must simultaneously be worked across national lines as well. Moreover, the dimensions of the integration challenge must be scoped to embrace all of the performance domains listed in Figure 3.

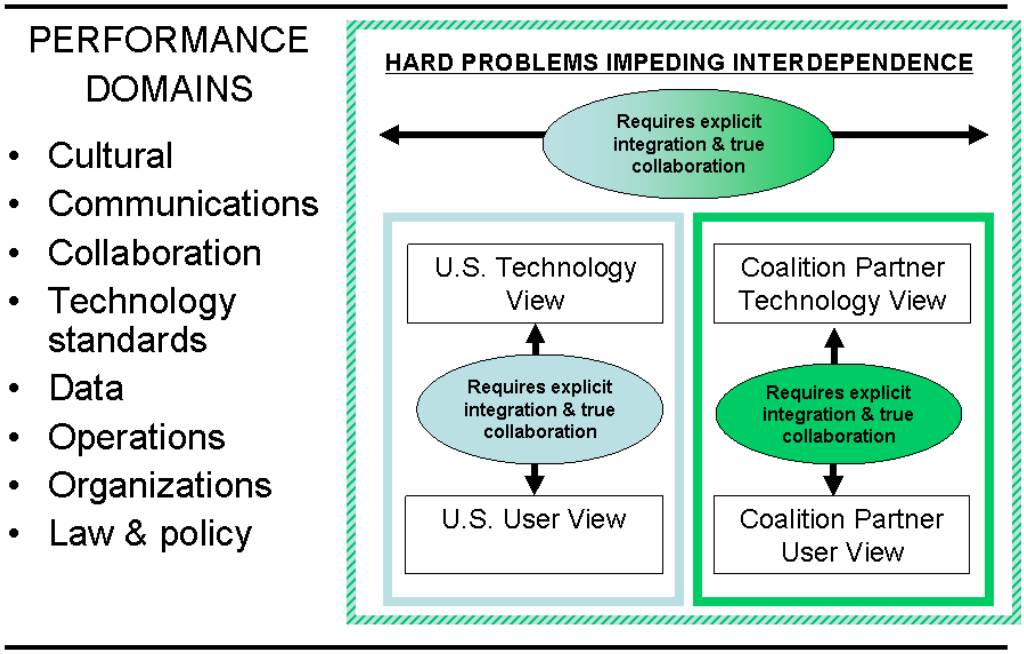

Figure 3. Universal framework for U.S.-coalition partner interdependent operations

To work just the simple impediments to performance is to surrender before the fight to the challenge of interdependence. Interoperability efforts tend to attack only a subset of the listed performance domains—technology standards, data, and communications. However, the two events that we ran showed that each performance domain is vital to developing U.S.-CP force capabilities that can deliver the interdependence that future forward commanders and decision-makers need.

To illustrate, the core problem, observed in both events, was the inability to conduct controlled information sharing in shared resource environments. To address this pervasive impediment to performance requires that two strategic challenges be recognized: 1) combat information sharing performance is out of alignment with network-centric expectations, and this must be accepted as fact if it is to be resolved; and 2) interdependence mandates the building of a sustainable network-centric solution that embraces, up front, the need to explicitly integrate technology, humans, and procedures. Recognizing that each nation's man-machine mix will be forever different, due to cultural perspectives, investment in defense, and other factors therefore requires development of a secure, universally adaptive "interface" capability suite that both facilitates and optimizes cross-nation peer-to-peer transactions.

In a technology sense, such a capability is needed to eliminate the current isolation of coalition partners from the network so that network benefits can be extended to each such partner. Today's approach toward building networks that are open to coalition partners is to add them on a case-by-case basis and modify the technology infrastructure accordingly. Players, especially at the U.S.-only workshop, observed that the technology challenge is not so much a challenge of securing the network, a la present efforts embodied in such architecturally-oriented efforts as the U.S.-developed coalition network called CENTRIXS, but instead a challenge to concentrate on technology approaches that seek to secure the data.

The adoption of such a mindset might be billed as the adoption of a need-to-share approach versus the current need-to-know approach. We hasten to add that this does not mean that information would be freely exchanged without regard for each nation's security protocols. Rather, it is offered as an explicit way to make the statement that in a U.S.-CP operational environment, there must be a concerted technology, policy, and operational commitment to provide each partner what they need to fight, not individually, but as a team. The need-to-know paradigm is important, but it should not continue to be used as a constraint against taking important actions to facilitate essential cross-nation information sharing. To illustrate, U.S. forces routinely operate with multiple nations in coalition partnerships. Yet, U.S. policy regarding the sharing of information is constructed on a country-by-country basis. Although provisions exist for commanders to make decisions to share at the "time of need," passive policy community engagement effectively precludes innovative technology and operational approaches from being worked by other than the on-site operator.

To underscore the centrality of information sharing to effective network-centric operations, recall that a basic objective of DoD transformation is forces that are "capable of rapid decision superiority." Decision superiority requires essentially three things: information and data availability, access to it, and decision support tools and related capability—all of which must be able to brought to bear in time to influence the action or decision-making of all coalition partners who are party to the action or decision in question.

Although information sharing was the core problem that impedes coalition-wide effective, interdependent performance, its implications touch most other issues that surfaced during the two experimental events. The inability to share and trust information also has implications for the development of effective cross-nation battle command. Battle command systems generally are characterized by databases and associated standards, mission planning and execution monitoring, and appropriate real-time cross-nation connectivity to each others' weapon systems and sensor capabilities. Each of those capabilities is to some degree influenced directly or indirectly by the information sharing challenge discussed above. But there are also other dimensions to battle command that are part of the challenge. One of these surfaced during the Singapore wargame where the commander of the coalition task force (CTF) granted operational control (OPCON) of a U.S. UAV to the coalition partner. During the game play, the players of the two brigades collaborated and mutually agreed to grant sensor control to the Singaporean Armed Forces (SAF) brigade while retaining platform control in U.S. hands. This was a reasonable approach in the context of the operational tasks and dilemmas being investigated but it surfaced one of several specific problems that will require both technology and operational community partnership to arrive at sustainable, effective solutions.

Cultural perspectives, although intangible, were observed especially in the U.S.-CP wargame as real factors that could have devastating operational consequences if not addressed. For example, rules of engagement (ROE) generally grant U.S. forces authority to take action based on hostile "intent." We found during the second event that SAF authority to act was predicated upon hostile "action." If one considers the possibility for multiple interpretations of the same adversary action by different coalition members, as was the case during the U.S.-SAF wargame, impediments to effective interdependent cross-nation performance are not difficult to envision. Solutions to dilemmas like this one do not seem to be technology intensive, yet technology may help to resolve this and similar issues if worked in an experimental venue with appropriate operators and policy-makers.

4. CONCLUSION

The transition to network centric warfare brings with it great promise for the effectiveness of future military operations, but along with this promise comes a variety of challenges. One of the most pressing and daunting of these challenges is achieving a network-centric, interdependent force with coalition partners. The challenge of interdependence is especially acute where there are differences in culture, technology standards, organization and doctrine, and policy and law that must be simultaneously managed in order to achieve a network-centric force. To begin the process of addressing the many issues that arise in coalition network-centric operations, two events were conducted by the Institute for Defense Analyses to explore the prerequisites for effective future U.S.-coalition partner military operations.

Clearly, the complexity associated with enabling effective and interdependent U.S.-CP operations provides a mandate for research to explicitly integrate man and machine and to do so across each performance domain. The complexity of the research task means is that no one organization, user, technology developer or nation can work the challenge alone. Structured, quick-turn experimentation that investigates specific issues of interest to specific operational communities—scenarios, missions, tasks—must be undertaken without delay and upon completion must be the basis for follow-on spiral development of not just technology, but importantly policy and new operational techniques and doctrine as well. The achievement of net-centricity, more than any other aspect of DoD's transformation, demands that the integration of man and machine be worked as a whole package that must succeed in an operational setting if the promised benefits of network-centric warfare are to be realized.

DISCLAIMER. The views are those of the authors only.

REFERENCES

[1] Department of Defense, *Transformation Planning Guidance*, Washington, D.C., April 2003.

[2] John W. Smith, Institute for Defense Analyses, *Setting the Conditions for Department of Defense Transformation: On Track to Support Future Joint Operations in Network-Centric Warfare?* Document D-2909, September 2003. This document also provides a fuller discussion of command and control versus battle command as well as a fuller discussion of interoperability versus the still-undefined term, interdependence. That discussion also provides the Defense definitions of interoperability.