This product is part of the RAND Corporation monograph series. RAND monographs present major research findings that address the challenges facing the public and private sectors. All RAND monographs undergo rigorous peer review to ensure high standards for research quality and objectivity.

Army Network-Enabled Operations

Expectations, Performance, and Opportunities for Future Improvements

Timothy M. Bonds, John E. Peters, Endy Y. Min,
Lionel A. Galway, Jordan R. Fischbach, Eric Stephen Gons,
Garrett D. Heath, Jean M. Jones

Prepared for the United States Army

ARROYO CENTER

The research described in this report was sponsored by the United States Army under Contract No. W74V8H-06-C-0001.

Library of Congress Cataloging-in-Publication Data

Army network-enabled operations : expectations, performance, and opportunities for future improvements / Timothy M. Bonds ... [et al.].
p. cm.
Includes bibliographical references.
ISBN 978-0-8330-4683-3 (pbk.)
1. Communications, Military—United States. 2. Information networks—United States. 3. United States. Army—Computer networks. 4. United States. Army—Evaluation. 5. United States. Army—Operational readiness. 6. Command and control systems—United States. 7. Military intelligence—United States. 8. United States. Army—Maneuvers. 9. Logistics. 10. Military art and science—United States. I. Bonds, Tim, 1962-

UA943.A76 2012
355.4—dc22

2009008950

Cover photos courtesy of (top left to bottom right) Spc. Alfredo Jimenz, Jr.; 1st Lt. Tomas Rofkahr; U.S. Army; Russ Meseroll.

Published 2012 by the RAND Corporation
1776 Main Street, P.O. Box 2138, Santa Monica, CA 90407-2138
1200 South Hayes Street, Arlington, VA 22202-5050
4570 Fifth Avenue, Suite 600, Pittsburgh, PA 15213-2665
RAND URL: http://www.rand.org
To order RAND documents or to obtain additional information, contact
Distribution Services: Telephone: (310) 451-7002;
Fax: (310) 451-6915; Email: order@rand.org

Summary

The U.S. Army expects that the performance of ground forces can be greatly enhanced by improving the networks that tie them together—and by developing new tactics that take advantage of the special properties of these networks. The Army employs literally thousands of individual networks, including those used by the operating forces for command and control, intelligence, maneuver, fires, and logistics, as well as those used by the generating force at bases in the continental United States and abroad.[1] These networks include the infostructure and services that process, store, and transport the information used by the Army.[2] Ultimately, then, these networks extend into the minds of soldiers and leaders and into their interactions with each other. In this monograph, we examine the capabilities that this broad set of networks provides in four areas:[3]

- physical aspects, including the radios, terminals, routers, landlines, and so forth that constitute the network infrastructure and provide network connectivity
- the information environment, including the databases where information is created, manipulated, and shared

[1] LandWarNet is the name that the Army uses for all of its networks (see Boutelle, 2004).

[2] U.S. Army Training and Doctrine Command (TRADOC) (2006a).

[3] TRADOC groups the first two categories into the Technical Area, and the third and fourth categories into the Knowledge Area (see Vane, 2007). These areas closely compare with the domains described by Alberts, Gartska, and Stein (1999).

- cognitive attributes, including sense-making tools that aid or enable situational awareness, situational understanding, decision-making, and planning
- social interaction, including collaboration, synchronization of actions, standard operating procedures, and tactics, techniques, and procedures enabled by the network.

One advantage that the Army hopes to gain from improved networks is the "quality of firsts," the ability to "see first, understand first, act first, and finish decisively." This concept entered development when the U.S. military was focused on major combat operations (MCOs). This study also assessed the degree to which networks can provide these same qualities to stability, security, transition, and reconstruction (SSTR) operations, counterinsurgency (COIN) operations, and warfare against irregular forces.

Specifically, this study addressed the following questions:

- Do the networks used by the Army enable commanders to "see first, understand first, act first, and finish decisively" and otherwise get forces and effects to the right place at the right time?
- What new, and perhaps unexpected, developments should the Army embrace and push forward?
- Where (that is, in what areas of the network) would additional investments yield the greatest rewards in terms of added performance?
- What changes in doctrine, organization, training, materiel, leadership and education, personnel, and facilities (DOTMLPF) should the Army make to achieve the expected network functionality and utility?

Conclusions

Our analysis of operations in Iraq, unit performance at the National Training Center and Joint Readiness Training Center, and officer impressions of network functionality led us to the following conclusions.

Army Networks Enabled the "Quality of Firsts" for Senior Army Tactical Echelons During Major Combat Operations

The ability of U.S. forces to gather, process, and disseminate battlespace information in a networked fashion has given them a tremendous advantage in MCOs. This dominant battlespace information has allowed U.S. forces to move faster and apply military power more aggressively and more effectively than their adversaries. Today's networks enable several key operational capabilities:

- shared situational awareness of U.S. forces, although a current or complete red picture was sometimes not available to echelons below brigade
- unity of action between U.S. forces
  - superior coordination and synchronization of U.S. forces when on the offensive—that is, when they have the initiative
  - promising instances of excellent coordination and synchronization when reacting to enemy actions or attacks
- enhanced shared understanding.

The most significant problem noted during past MCOs was an incomplete or dated view of red forces. New investments, such as unmanned aircraft systems and the Distributed Common Ground System–Army (DCGS-A), may help to improve red force information available to lower echelons.

Army Networks Have Not Yet Enabled the Same "Quality of Firsts" for SSTR Operations, COIN, and Irregular Warfare

Today's networks do not yet enable all of the force-enhancing effects that the Army expects:

- Army units often do not see first or act first when enemies use irregular tactics.
  - Many reconnaissance, surveillance, and information systems were developed to find conventional armies when U.S. forces have the initiative.

  - They are less effective in detecting and identifying irregular enemies before they initiate attacks.
  - Information superiority in COIN and irregular warfare can therefore shift from U.S. forces to insurgents.

The Army's current networks do not yet enable seeing first or understanding first in all SSTR, COIN, and irregular warfare operations. The networks enable situational awareness of other blue units but do not always provide reliable awareness of red units before they attack, which is much more challenging. The networks do generally support reactive tactical coordination and unity of action, thereby allowing units to usually finish decisively.

Soldiers and Leaders Are Informally Linking Networks Together to Enhance Their Effectiveness

Our officer survey data revealed the following:

- Informal networks—often hosted on SIPRNet (Secret Internet Protocol Network)—received the highest ratings of all the networks.
- SIPRNet was rated as better than the other systems at establishing shared situational awareness with U.S. forces.
- But key systems—e.g., SIPRNet, FBCB2 (Force XXI Battle Command Brigade and Below), and CPOF (Command Post of the Future)—are not typically shared with coalition and host nation units.

Officers we surveyed viewed the SIPRNet as the best tool for establishing situational awareness between U.S. units. Where available, the SIPRNet was an essential means of connecting soldiers and leaders with sensitive databases and other sources of information within theater or elsewhere in the world. Unfortunately the SIPRNet and other networks such as FBCB2 are not typically shared with coalition or host-nation units nor are network-enabled tools such as CPOF.

The case studies and surveys we conducted reveal that soldiers and leaders are investing time and unit resources in informal networks that connect and fill gaps in the formal networks. These include unit-

level databases to gather information from (and for) local operations; user applications to sort, search, and make sense of these data (that is, cognitive aids); and social networks to share this knowledge with peers brigade-, division-, and corps-wide. The blogs, online discussion groups, and chat rooms prompted by such shared application have spawned an important "social domain" of the network to enhance the effectiveness of unit, task-force, or theater-wide operations.

Opportunities Are Emerging for the Army to Enhance Future Operations Through Improvements in the Networks' Social and Cognitive Domains

We saw significant potential to enhance the effectiveness of U.S. and coalition forces by providing networks that can enable

- adjacent U.S. units to self-synchronize
- command posts and higher headquarters to provide "electronic overwatch."

As noted in this monograph, ground forces are putting more and more information onto SIPRNet, FBCB2, CPOF, and other networks that can be used to synchronize the operations of adjacent units and units that are moving adjacent to one another. Often, this information can be updated automatically, without placing additional obligations on already overtaxed command post staffs. For example, the movement tickets that convoys are supposed to generate before departure could be pushed automatically to the headquarters of each area of operation (AO) that a convoy will move through. These trip tickets, along with information broadcast en route over SLANT reports, would provide a way to synchronize the convoy with those forces it will move adjacent to. Similarly, any moving air or ground unit could synchronize its activities with other U.S. forces that it approaches in the battlespace.

Additional advantages may be gained when networks enable electronic overwatch. Command posts that are synchronized with lower-echelon forces in their areas of operation may be in the best position to provide support (such as intelligence, fire support, or even a quick-reaction force) to these forces when they most need it. Having the nec-

essary connections, tools, knowledge, and mindset may allow these command posts to enhance the effectiveness of these units at critical moments.

Recommendations

The Army has made substantial investments in the network with the intention of achieving network-enabled operations. Indeed, the rubric "see first, understand first, act first, and finish decisively" has become pervasive in current and future concepts. Assuming that the Army continues to believe that the network and network-enabled operations can deliver enhanced battlefield performance, we recommend that the Army pursue the network objectives described below.

Continue and Expand Efforts to Extend the Network to Lower Echelons

At the tip of the spear, small units experience limited network access and capabilities. Often, platoons and squads are operating on the move or in combat outposts far from other units and lack direct access to intelligence, surveillance, and reconnaissance data. Current plans to distribute unmanned aerial vehicles (UAVs) downward through the brigade combat teams are a step in the right direction, along with direct-downlink terminals. In addition, providing the DCGS-A down to battalion and company levels will help. The key future challenge will be maintaining these connections to units on the move and building display systems that enhance effectiveness during high-intensity operations. More recent initiatives to provide Human Terrain Teams, Cryptologic Support Teams, and other specialized support at echelons brigade and below should be continued.

Many of the officers who responded to the project's surveys called for forward distribution of a SIPRNet-like Web-based classified system to lower-echelon units. SIPRNet is now reaching some company-level units at fixed sites, but platoons are increasingly assigned to man remote outposts. Where appropriate, the Army should develop the means to provide secret channels down to the lowest level of iso-

lated units. Where this is not possible (because of operational security [OPSEC] concerns, limited bandwidth, and so forth), their higher headquarters should provide electronic overwatch.

One aspect of extending the network should be to extend its capabilities to identify the enemy before the shooting starts. The Army should intensify its efforts to expand its reconnaissance tools. In addition to the efforts under way, the Army might also consider emblematics, more biometrics, and new ways of instrumenting the battlespace that would reveal enemy combatants and their organizations. Another aspect of extending the network would be to take advantage of current intelligence, surveillance, and reconnaisance "feeds" by distributing them down the chain of command to smaller units that could use this information as context for understanding the clues they are collecting about the enemy within their own area of operations.

Invest More Time in Developing and Exploiting Informal Networks

Officer survey responses indicate that informal networks perform important functions within and among deployed units. It appears that they may fill gaps in information and connectivity not provided by the formal network. The Army has supported some of these soldier initiatives—and should strive to study and harness these networks as they emerge. The G-6 and G-3 will want to coordinate closely to begin thinking about how to manage the intersection of systems of record with informal networking practices and how insights from such a process might inform network design and battle command practices.

Expand the Network to Include All Important Actors

A central tenet of irregular warfare is that the military provides only part of the solution. The host nation, coalition partners, other U.S. executive branch agencies (such as the State Department and U.S. Agency for International Development), international agencies, and nongovernmental organizations (NGOs) must be included. Expanding the network to include such a wide range of coalition partners clearly presents issues about OPSEC and information security, but there are some precedents for handling them. The Combined Enterprise Regional Information Exchange (CENTRIX) network, despite its limitations,

suggests one way to undertake extended connectivity and share "rapid decay" current intelligence, since it makes enemy exploitation of leaked intelligence difficult. This would also promote unity of effort and good faith with any number of participants.

Still, some nations, NGOs, and individuals may require extensive vetting over considerable periods of time. It may be necessary to continue the Special Forces practice of using unclassified, commercial radios and computers to connect these groups and individuals with U.S. forces—recognizing that these communications are very likely to be intercepted.

Enact DOTMLPF Changes to Enable Self-Synchronization and Electronic Overwatch

The Army should consider the following DOTMLPF changes to implement our recommendations:

- Doctrine
  - Help platoons and squads when they are operating alone against irregular or hidden forces. Doctrine needs to allow and encourage adjacent units to self-synchronize information, plans, and capabilities while executing their assigned missions.
  - Assign overwatch duty to an adjacent unit when it is in a tactical situation that allows it to provide support.
- Organization
  - Provide designated headquarters and command posts with the appropriate staff, network tools, and training to conduct electronic overwatch.
- Training
  - Provide training to implement self-synchronization and electronic overwatch.
- Materiel
  - *SIPRNet:* Provide SIPRNet down to the platoon level if these echelons continue to man combat outposts.
  - *Blue force location, identification, tracking, and synchronization:* Provide real-time blue force tracking to every unit that con-

ducts independent operations. (Also, provide the best red force picture possible on this equipment.)
  - *Intelligence, surveillance, and reconnaissance systems:* Continue to provide an organic way to access intelligence, such as direct unmanned aircraft system downlinks and DCGS-A. Enable electronic overwatch over voice and text systems for those echelons not able to receive DCGS-A.
- Leadership and Personnel
  - Encourage soldiers and leaders to develop and use such sites as the CompanyCommand Forum and CavNet as places to meet, learn, and build new concepts.
  - Reward soldiers and leaders who develop new applications to tap into the multitude of classified databases to gather intelligence concerning recent enemy movements, attacks, and other activities.