

*A Primer on U.S. Military Ground Forces'
Wireless Communications Requirements and Recent Lessons Learned*

Michael Bowman PhD, Murray State University; and Gregg Petersen, Cypress International, Inc.

International Telecommunications Education and Research Association (ITERA)

Fourth Annual Conference on Telecommunications & Information Technology

March 19-20, 2006, Las Vegas, Nevada, USA.

Scenario

You are a U.S. Army or Marine Corps Colonel and a brigade commander. It's 96 hours into a major, regional, high-intensity conflict. You are directly responsible for the 2500+ members of your brigade combat team and their mission as the spearhead of a coalition offensive thrust into enemy territory. Your troops have moved fast and aggressively to seize their objective - a bridge across a major river, along one of several lines of advance that might be used by the coalition. On one-hand your mission has been a resounding success, as you have captured the bridge with a minimum of casualties. On the other-hand, you are now more than 30 miles out in front of the bulk of coalition forces and you, and most of your troops, have not eaten, slept, or been re-supplied adequately for more than 100 hours. It's up to you to decide what to do next: continue to advance; pause in place in your offensive posture; or switch over to the defense while follow-on forces catch up.

If this were 1991, before the development and adoption of robust military "situational awareness" systems you might be mostly lost in the "fog of war," the confusion that results from the smoke, noise, fear, and uncertainty of combat. You would have only a limited ability to directly see your forces arrayed around you. You would have partial information about the far-flung locations of your subordinate commanders and their troops based on spotty and infrequent

radio reports. The reports arrive at different times and on different radio nets. The reports might be scribbled down on scraps of paper and passed to you; or transferred to acetate overlays on your paper maps by your staff; or simply arrive simultaneously as low quality audio over any of several speakers that you are trying to listen too. The age and accuracy of the reports you receive would be highly suspect – they come from soldiers, mostly using maps and compasses to assess their self location while operating under great stress in a hostile environment. You know much less about enemy forces. It's doubtful that you have, or ever will directly see the enemy. Your scouts move aggressively across the battlefield to find the enemy but it's a tough task, and subject to similar but even more challenging reporting problems than you have in getting friendly force information. You know that coalition forces are working hard to collect and analyze information about the enemy but duplicate sightings of the same unit; limited communications systems; security barriers; and poor dissemination processes make it unlikely that much of this information will reach you in an accurate or timely manner. Further, your ability to directly communicate with your subordinates, and to your higher headquarters, is severely limited by your rapid movement, the long distances involved, and your reliance on line-of-sight communications systems.

If instead, this is 2005 and your brigade is equipped and trained to use the emerging “situational awareness” systems of U.S. ground forces, and conducting “network centric” operations, your situation might be radically different. You still have a limited ability to directly see your troops, but now you have very good information about where they are, based on “blue-force-tracking” (BFT) and “global positioning systems” (GPS). Most of your 500 vehicles are now equipped with GPS. The GPS determines a vehicle's location every few seconds and automatically reports the vehicle ID and location to your command vehicle or command post

through the communications hardware of the BFT systems. These locations are then automatically plotted on a digital map on a computer display for you. Enemy locations identified by your scouts, now much more accurate because the scouts accurately know their own location, are reported to you in a similar manner. New line-of-sight (LOS) and beyond-line-of-sight (BLOS) communications systems give you a much greater ability to communicate with your troops and your higher headquarters via digital voice and messaging. Information about enemy locations, collected by a host of intelligence systems are now automatically disseminated and displayed on your computer screen, including video images collected by the cameras of your brigade's unmanned aerial vehicles (UAV) and transferred to your display by a tactical internet.

This scenario is in fact exactly what a U.S. commander faced in the opening days of the 2003 conflict in Iraq. When his brigade seized the objective bridge, his command, control, communications, and computer (C4) systems told him how his brigade was arrayed around him at the bridgehead. Further, his C4 systems told him that the coalition forces that were supposed to use the bridge to continue the attack were still several hours away. Most importantly, as the situation continued to develop, his systems told him that a large enemy force was advancing toward the bridge from the far side. Quickly assessing the situation, the brigade switched over to a defensive posture; rapidly prepared and disseminated defensive battle plans; and coordinated for support from other coalition air and ground forces. The brigade was subsequently successful in repelling the attack of the larger enemy force, and able to rapidly switch back over to the attack (Lawlor 2005). If the brigade had continued its initial advance, or had not switched into a defensive posture, the ensuing battle might have had a disastrous outcome for them. The unit's communications and automated command and control systems played a pivotal role in this battle and contributed in a significant way to the successful outcome.

New Market Realities

Since the invention of wireless communications more than a century ago, the military has very often been at the forefront of leading-edge application of the technology. Today the commercial sector has overtaken the military in terms of first-use and high volume/density application of emerging technology and standards such as IEEE 802.xx protocol wireless communications (Hawk, 2005). None-the-less, military forces throughout the world, and the U.S. military in particular remain a major market for modern communications technology, in an environment where robust and reliable wireless communications can be a matter of life and death. At the dawn of the 21st Century the U.S. military has committed to major investments in modern wireless communications as a center-piece for network centric operations, and to provide “situational awareness” to “lift the fog-of-war” for committed forces.

Network-Centric Operations

Network-centric military operations are operations enabled by networking military forces to provide an integrated picture of the battlefield, available in detail at all levels, down to the individual soldier. This extensive information sharing and synchronization is to be achieved by equipping command posts, vehicles, and individual soldiers with computers and displays, all linked by wireless, radio-frequency networks (Wesenten, et al, 2005). The effectiveness of network-centric operations will depend upon the availability and dissemination of information on the status and disposition of friendly forces, enemy forces, and other critical aspects of the operational environment displayed as icons on digital maps on a computer screen. The underlying assumption is that this information sharing and synchronization leads to situational understanding, rapid decision making, and proactive operations that can constitute a decisive warfighting advantage (Cebrowski & Garstka, 1998).

Situational Awareness

In layman's terms, situational awareness has three components: knowing one's own location; knowing the location of nearby friendly forces; and knowing the location of nearby enemy forces. Self location comes through the widespread use of Global Positioning System (GPS) receivers. Awareness of the location of nearby friendly forces comes through widespread pairing of GPS with transceivers in military vehicles and small units that broadcast encrypted identity and location information to other friendly units. Awareness of enemy location comes through the collection, analysis, and automated dissemination of intelligence on the enemy forces. All three of these pieces of information are then viewed as icons overlaid on digital maps displayed on rugged, portable computers. Beginning in the early 1990s, the U.S. Army incrementally developed, experimented with, and fielded a situational awareness system named Force XXI Battle Command Brigade and Below (FBCB2) which used Enhanced Position Location Reporting System (EPLRS) LOS communications for information sharing. In the late 1990s, to support rapidly emerging requirements for tracking patrols conducting peacekeeping operations in the Balkans, a lower cost, nearly off-the-shelf, "Blue Force Tracking" system based on commercial Ku-band satellite transceivers was fielded and integrated with FBCB2 capabilities to form the predecessor of today's L-band FBCB2-BFT system deployed in South West Asia. A variety of studies and reports over the last five years, including looks at lessons learned from high and low intensity combat operations in Iraq, cite up to a ten-fold increase in combat effectiveness in military units due to the current level of networking, and there are high hopes for greater improvements as new systems and technologies to integrate other Service and National BFT systems become available (Lawlor, 2005). These results are not a surprise. The severe impact of the fog-of-war, and the need to improve communications in combat to help lift the fog,

has been a well-established theme for several centuries. The Army's BLOS FBCB2-BFT system and its use in U.S. Military Forces still faces challenges. It is not fully interoperable with a similar U.S. Marine Corps system called the Mobile Data-Automated Communications Terminal (M-DACT) or all Air Force platforms, but that is being worked on (Dervarics, 2005). The U.S. Air Force has begun installing an FBCB2 interface on its Joint Surveillance Target Attack Radar Systems (JSTARS) aircraft. With this interface installed and operational, the aircraft will receive regular updates from the FBCB2 system, and send the blue force data to each of the JSTARS work stations, where the information is overlaid on existing displays. It gives the JSTARS operators the opportunity to associate FBCB2 data with real-time ground moving target indication, or GMTI data, that the aircraft collects (Fox, 2006). Other BFT systems that have value but have integration challenges with the Army's BLOS BFT system include its own logistics Movement Tracking System, Orbcomm GeoTrac products, Grenadier BRAT (BLOS Reporting and Tracking) and its man-portable MTX system, and the Air Force's TALON REACH.

The need for situational awareness as the center piece of network-centric military operations, as well as all the fundamental information requirements necessary for military command, control, intelligence, and logistics functions, means the military will continue to be a huge consumer of bandwidth and communications hardware.

A Global Communications Task

A discussion of current U.S. Military communications requirements can start with two primary dimensional concepts: an x-axis of "Whitehouse-to-foxhole" communications; and a y-axis of "space-to-mud" supporting communication systems. That is, military commanders require and expect to communicate globally, from the Whitehouse to the most remote soldier's foxhole; and

they are prepared to use layered space-to-mud communication systems to accomplish this task. The U.S. Military already can and does communicate from the Whitehouse to “selected” remote foxholes when the situation warrants the connection and time allows the links to be established. They just can not communicate to all foxholes, all the time, and not without significant set up times to establish the Whitehouse-to-space-to-mud links. This is primarily due to hardware and bandwidth limitations on the foxhole side of the axis.

Problematically, at the same time that it is possible to communicate from the Whitehouse to a given foxhole, there are situations where communications can not be established or maintained from one foxhole to the next. Lack of transceivers in every foxhole, incompatible transceivers, incongruent encryption systems, incongruent network addressing schemes, intervening terrain that breaks the line-of-sight, lack of relay systems to extend line-of-sight, low densities of non-line-of-sight systems, power requirements, and system complexity all contribute to today’s situation where it is still not always possible for two adjacent soldiers or units to communicate adequately.

The Old Acquisition Strategy

For at least as long as the military has been using radios to support operations, there has been a desire to have homogenous voice and data communications networks with common, ubiquitous transceiver hardware and net management systems. Given widely diverse requirements sets, long development times for new technology, and low funding levels that drive slow acquisition and fielding rates, the goal of a homogenous communications system has never been achieved. There are always units using legacy, prior-generation systems long after other units have received new technology. This absolutely remains true for the U.S. Military today, and is

compounded dramatically when current and potential coalition and allied partner's needs for interoperability are considered in the mix.

This theme and problem persists today with ponderous, developmental military acquisition programs such as the U.S. Joint Tactical Radio System (JTRS) which was intended to provide software programmable common radios across a wide spectrum of military requirements, broken down into a small set of radio "classes." Most especially however, this program was meant to provide wideband wireless capability to troops and commanders conducting and supporting the maneuver battle. The desire to provide a minimum variety of radio types to meet a vast range of requirements and the high technical risk for "bleeding" edge software programmable technology has caused the program to be often delayed and plagued with the resultant higher costs associated with those delays and the high complexity. Further, by aiming to please all users, all of the time, the program has failed to meet users' expectations in terms of schedule, cost, size, weight and power consumption of the future radios. When the Defense Department documented its expectations eight years ago in its Operational Requirements Document (ORD), despite being dependent on commercial sector technology advances, it had no crystal ball to predict that nearly 5 ½ Moore's Law cycles later that 802.11 technology and Internet Protocol (IP) wireless technology would likely be the effective, practical, ubiquitous solution to their wideband needs vice one of over thirty "waveforms" in software programmable radios.

A New Acquisition Strategy

Given these issues regarding technology cycles and cost, a new acquisition and system management model is gaining support in the military in the high technology areas of Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance (C4ISR).

First, as previously stated, this new model recognizes that the military is most often not driving the market for new communications technologies and standards and will often only adopt a new technology or standard after it has become a winner in the commercial sector. Next, while still striving to minimize the variety, and maximize the commonality of systems in use in the military at any given time, the military recognizes that ultimately one size does not fit all and evolutionary technology integration is preferable and more cost effective in contrast to long developmental cycles. At the same time, a layered space-to-mud approach to communications tools will always be necessary to meet its diverse requirements. Finally, rather than focusing on the large, slow, expensive “big bang” communication systems acquisition programs, some now argue for shifting focus and resources to mastering the “rapid connecting and integration” of the communication systems we have now with rapidly developed, commercial-products based, state-of-the-shelf communications systems. Rejecting the concept of building a single, global, end-to-end system over a decade or more, the new strategy calls instead for grinding out an evolving, consistent, regular series of rapidly developed and fielded network segments and nodes, that include state-of-the-shelf, highly flexible, and high capacity connection devices – bridges, routers, network nodes, and terminals. Recognizing that it is often the configuration and management systems that make the set-up and operation of today’s networks possible, equal priority would be placed on these software components as given to the hardware components.

The integration of FBCB2 and the L-band commercial-product based BFT and its successful use in numerous conflicts is cited as a positive example of this new “connect and integrate” focus. Rather than sticking solely to the established program, or completely dumping the mil-spec program to adopt a new commercial system, the best of both systems have been adopted and used where they best fit the overall requirements. An example of this new strategy

of focusing on the “connecting” of systems as demonstrated in the U.S. Army’s Joint Network Node (JNN) is described below.

An Example of the New Acquisition Model

The U.S. Army’s Joint Network Node (JNN) is a prime example of this new military communications acquisition strategy. In the post 9/11 environment, the U.S. Military has placed an extremely high priority on being able to rapidly deploy ground forces around the globe on short notice with sufficient organic communications capability. Shortfalls in current communications equipment and organizations became even more evident during the preparations and planning for the early 2003 phase of the Iraq conflict. In response to the “good enough” integration efforts leading up to and during the combat operations of Operation Iraqi Freedom (OIF), the Army built the JNN architecture over just a twelve month period to fill immediate communications shortfalls in its maneuver brigades and higher level commands.

The JNN is an off-the-shelf, government and commercial-equipment based architecture to provide Army brigade and higher units organic, BLOS global communications links, and significantly improving local communications and networking. It provides Internet Protocol (IP) based voice, data, and video conferencing capability supported by Ku/KA satellite technology.

The JNN architecture includes three primary component systems: A Unit Hub Node (UHN) provides satellite connection management for all elements of a unit’s network and acts as a base-band or tactical technical node facility; a Time Division Multiple Access (TDMA) satellite network for intra-unit BLOS connectivity; and a Frequency Division Multiple Access (FDMA) satellite network for long range BLOS connectivity to the U.S. Department of Defense Information Systems Network (DISN) Global Information Grid (GIG) architecture (Edwards, 2005).

To support brigade and battalion tactical internets the JNN includes 2651 and 3725 series routers, 2950 and 3750 Ethernet switches, and VG248 gateway voice equipment from Cisco; Promina 400 broad-band services delivery platforms from net.com; HDX PBX switches from Redcom; and NetScreen 25 and 5XT firewalls from Juniper. The system also uses the General Dynamics' Vantage gateway, which lets it share information with legacy communications systems.

In line with the new acquisition strategy outlined above, the JNN is still a work in progress. The initial architecture has been both praised and criticized by troops in the field and the architecture is being modified to overcome identified shortcomings and expand capabilities.

Military logistics processes have been augmented in a similar, very effective fashion as military units receive Very Small Aperture Terminal (VSAT) satellite BLOS communications systems to provide their supply and sustainment elements the much needed bandwidth and connectivity required for them to become network-enabled.

Lessons Learned and Near Term Communications Priorities from Current Operations

Communication lessons learned coming out of U.S. ground forces in Iraq and Afghanistan hold few surprises. Mostly, they call for capabilities the military recognized were needed, but did not have ready technology for, or could not afford.

Some persistent truths are sustained by the lessons learned.

- There is no such thing as perfect situational awareness as combat is a dirty, confusing, dangerous activity.
- Close combat will not be eliminated through good situational awareness, but having situational awareness does represent a significant tactical advantage.
- Ground forces should be “network enabled” not “network dependent.”

- In the end, the network is a critical component of the sum that is combat power.
- In close combat, well trained troops, volume of fire, marksmanship, and leadership still win the day.

Improvements to Situational Awareness / Blue Force Tracking Despite the undisputed success and importance of situational awareness through BFT, it is still available and distributed in too low a density, with too many versions, and too little integration across the entire friendly force. As stated above, there are still Army units that don't see their nearby Marine counterparts; coalition ground forces are rarely integrated; and there are far too many attack aircraft that do not receive and display the locations of friendly ground forces. BFT has made significant contributions to reducing ground-to-ground fratricide, but the lack of BFT in most attack aircraft means it has not made a similarly important contribution to ending air-to-ground fratricide. Ironically, the Defense Department's efforts intended to fix communications interoperability problems through the JTRS solution in the long term, curtailed the acquisition of the Situation Awareness Data Link (SADL) to all but a very few close air support aircraft in the short term, when this capability would have been useful in Iraq. SADL is interoperable with U.S. Army' and Marine' EPLRS and if the Defense Department had allowed the Air Force to acquire it in larger quantities, there would be much better visibility between Air Force attack aircraft and U.S. ground units in contact with the enemy during ongoing combat operations.

Improved BLOS Communications BLOS and satellite communications were relatively unheard of below division level just ten years ago. Fielding of JNN is pushing a satellite terminal down to every maneuver battalion but the requirement for BLOS communications will not be satisfied by a single link. Operations in mountainous, urban, or otherwise compartmented complex terrain where units in relatively close physical proximity are

not able to establish and maintain LOS communications is highly common in Afghanistan and Iraq. Simple, flexible, low cost BLOS capabilities are needed at a much higher density in combat units. Reduced size, weight, and power consumption; greater bandwidth and reliability; and reduced set-up and tear-down time are all desired in future BLOS communications systems.

Improved LOS Communications Radios will never be small enough, light weight enough, simple enough, or battery-efficient enough to satisfy the dismounted warfighter. Ground forces are looking for universal distribution of cell phone like personal communications devices. Deploying units routinely buy out the local commercial hand held radio market before departing their home stations. Use of these commercial products help units for only a short time before lack of encryption, repair, re-supply, and frequency management problems outstrip the benefit. The upside of the forecast for this area is that the more commercial companies focus their research and development on portable phones, portable music players, and portable gaming stations providing real-time webcasts and online gaming, the more capability will be available for spiral fielding to the dismounted soldier.

Communications Systems for Urban Environments, Underground, and Caves

Incorporating BLOS and/or LOS communications technology, warfighters need to communicate when they are in urban structures/urban canyons, triple canopy jungle, underground, or in caves. Current promising commercial technology in this area includes the 'Breadcrumbs' dropped repeater systems. In addition, the Department's JTRS efforts on the Soldier Radio Waveform (SRW) shows some initial useful capability to improve dismounted soldier communications in this challenging environment.

Improved GPS Extremely dense distribution of smaller, lighter weight, simpler GPS devices is necessary. Many soldiers still deploy with and rely on their personal commercial GPS

because of limited distribution of costly full-capability military versions. Department rules prohibit the wholesale purchase and provision of commercial devices to soldiers in favor of encoded and encrypted but expensive militarized GPS. Exceptional consideration of providing a commercial capability for non-critical targeting or location requirements would be practical and would provide “good enough” location information to all soldiers while saving them out-of-pocket costs. The fog-of-war and a lack of GPS made major contributions to PVT Jessica Lynch’s convoy becoming lost and ultimately ambushed. The story might have been different if each vehicle in her convoy had been equipped with a commercial GPS.

ISR integration and Communications There are greatly increased numbers and types of sensors on the modern battlefield such as UAVs, but the bandwidth available to get critical intelligence gathered by these sensors to the warfighters has not kept pace. Bandwidth, not sensor availability, is usually the limiting factor in how much timely intelligence a commander receives. Some sensors sit idle for lack of bandwidth. Further, available sensors are not adequately integrated with command and control systems. Rather than all intelligence from all sensors being networked to a few workstations in the command post, most sensors directly feed a dedicated, uniquely configured workstation. This results in large numbers of workstations to be operated and sustained, and makes manually intensive procedures necessary for transferring intelligence to the interested commander. In this domain where the information UAVs provide is time-critical and perishable in utility, greater interoperability and access for all commanders with a need is required. Further, analyzed and processed intelligence from the wide variety of available sources must be fused and made available in a searchable form so that commanders and leaders can use ‘Google’ like search capabilities to find critical information about the enemy.

Internet like access to all manners of information Our soldiers and younger leaders come from a “world wide web, cell phone, video game, iPod” society. They need and expect Internet like access to all manners of relative military information. They expect to be able to “Google” for every thing from enemy locations to the status of re-supply, and “instant message” the guy or girl in the next foxhole. When they can email their family and post updates to their personal blog from their Forward Operating Base (FOB) in the combat zone, they will never understand why they can’t get a spot report through to their commander during a firefight.

Systems to Meet some of the Near Term Needs

The Joint Global Communications Infrastructure To support the Whitehouse-to-foxhole communications which enable the U.S. to act rapidly around the globe, and still adequately command and control deployed forces, an ever more connected and integrated global communications and information infrastructure is required. This infrastructure has come to be called the U.S. Department of Defense (DoD) Global Information Grid (GIG). As defined in the U.S. DoD Directive 8100.1 the GIG is:

The globally interconnected, end-to-end set of information capabilities, associated processes, and personnel for collecting, processing, storing, disseminating and managing information on demand to warfighters, policy makers, and support personnel. The GIG includes all owned and leased communications and computing systems and services, software (including applications), data, security services, and other associated services necessary to achieve Information Superiority. It also includes National Security Systems as defined in section 5142 of the Clinger-Cohen Act of 1996 ... The GIG supports all Department of Defense, National Security, and related Intelligence Community missions and functions (strategic, operational, tactical, and

business), in war and in peace. The GIG provides capabilities from all operating locations (bases, posts, camps, stations, facilities, mobile platforms, and deployed sites). The GIG provides interfaces to coalition, allied, and non-DoD users and systems.

The intent is for the GIG to provide users with a seamless, secure, and interconnected world-wide information environment, which allows them to access data when ever they need it, from any location, without having to rely on, or wait for organizations that collect, process, store and disseminate the information (GAO, 2004). Based primarily on commercial communications and networking components the GIG currently has three major tiers consisting of: advanced “transformational” communications satellites; fixed and mobile multi-band ground stations; and the tactical internets of the military services. Literature often includes references to the “Defense Information Systems Network” (DISN), which is undergoing a major upgrade in the DISN-Bandwidth Expansion (DISN-BE) project, as the fore-runner of the GIG. Defense Department documentation emphasizes that the GIG is a communications infrastructure for connecting deployed and mobile military forces to the usually fixed communications infrastructure of the DISN.

The Army Tactical Communications Infrastructure The U.S. Army’s Warfighter Information Network – Tactical (WIN-T) program will implement the Army’s tactical portion of the GIG. WIN-T was initiated in the late 1990s because the Army’s existing tactical communications network for C4ISR could not adequately support network-centric warfare concepts or more than basic situational awareness. Experiments and lessons learned from ongoing combat operations show that ground forces require a much broader spectrum of information services than is currently available to them including: streaming video and audio

from sensors, multi-dimensional graphical data and imagery, collaborative planning tools, embedded synthetic environment training, tightly integrated C4ISR systems, and distributed databases.

To address these new requirements, WIN-T is designed to be a broadband, on-the-move enterprise and tactical intranet that will use commercial technologies for wired and wireless voice, data and video communications. Initial goals for on-the-move bandwidth capacity for vehicles traveling across rough terrain is 256 kilobits of data per second. A high priority has been placed on providing automated network management and maintenance features in WIN-T including dynamic bandwidth allocation for on-the-move satellite communications in self-healing, self-forming networks operating over Internet Protocol version 4 (IPv4) and Internet Protocol version 6 (IPv6).

Early WIN-T capabilities are already being tested. November and December 2005 WIN-T prototype demonstrations included on-the-move networking over terrestrial LOS and satellite BLOS links; voice, video, and data over IP; self-healing network characteristics; automatic satellite tracking and adaptive signal retrieval; network operations with real-time situational awareness; network security; secure cellular communications; and collaboration tools reaching from commanders to dismounted soldiers (Tiboni, 2005).

Longer Term Military Communications Requirements

On-the-move and Hands Free Communications U.S. Military doctrine is very clear in stating that rapid maneuver and aggressive offensive operations are critical to achieving success even in modern network-centric operations. This mandates that all the critical information and communications links commanders have access to in a fixed command post must be available while he or she is on-the-move. Today, commanders still leave too many critical systems and

communications links behind when they leave their command post and mount their fighting vehicle. The situation is dramatically worse, when they conduct dismounted operations.

Soldiers have only two hands, they can not fire their weapons, or operate their equipment, and still have hands free to operate communications gear.

Mobile Ad-hoc Networking (MANET) Great strides have been made in networking current military forces compared to even ten years ago. Despite the gains, establishing, operating, and changing those networks are currently complex, difficult, manpower intensive tasks. Future networks must have robust, automated network management systems that quickly establish ad hoc IP based networks, keep them operating on-the-move, and allow them to be regularly changed on-the-fly.

Imagine a military force assigned the mission to advance through enemy territory to link up with a special operations force that has seized a bridge. The force is to be augmented with reinforcements, and special purpose units to accomplish the mission. Local coalition forces join them to act as scouts and guides.

- As all the assigned units approach an assembly area their individual networks should automatically integrate with one another and be absorbed into a single organizational network.
- As the force moves out from the jump-off point, manned and unmanned aircraft moving in to and out off their sector automatically join and depart their network.
- Unattended, disposable ground sensors seeded along their route of advance enter their network and pass intelligence to them as long as they are within communications range.

- Throughout their approach toward the special operations unit at the objective bridge, airborne relay systems link the networks of the two forces to provide continuous situational awareness between them and prevent fratricide as the forces link up.

The Army has collocated a program manager with the Marines in Quantico and begun development and fielding of Mounted Battle Command on the Move (MBCOTM) prototypes to provide an initial capability for high priority mobile command nodes in its HMMWV, Stryker and Bradley vehicles. A dozen MBCOTM sets have been fielded recently in HMMWC configurations with another dozen+ expected in the next year.

Communications Relay UAV and Aerostat The U.S Military has recognized for many years the critical importance that airborne communications relay systems can play in extending the effective range and eliminating obstacles for LOS communications systems. Today the number of UAV and Aerostat systems is increasing steadily, yet none are regularly made available as communications relay platforms. High endurance, high altitude communications UAVs and Aerostats are more flexible and a fraction of the cost of satellites. Their regular, dedicated use by conventional ground forces is long overdue.

Disposable Communications for Disposable Sensors Future ground forces will want to make extensive use of inexpensive, disposable, remote ground sensors and small, hand launched UAVs. To support disposable sensors, extremely low cost, tamper proof, chip sized radios are needed to network them, and provide links to maneuvering forces. These radios will require an appropriately secure, yet minimal level of encryption protection that must be in keeping with the extremely low cost and disposable nature of the radios and the sensors they are integrated with. The current JTRS program has plans to provide a radio class roughly meeting

the size requirements for disposable radios, but it is unlikely to provide them at a cost or security classification that would make them suitable for use in a disposable sensor.

Multi-purpose Radio Frequency (RF) Systems A critical and central, long term, C4ISR priority for future ground forces is the development of multi-purpose RF systems. It is hoped that a single RF system on a future military platform can serve multiple critical purposes such as:

- High capacity communications;
- Combat identification discerning friend from foe;
- Threat warning functions that detect inbound projectiles in time for them to be countered; and
- Long range target identification.

Conclusion

Wireless communications systems have played a key role in military operations for over one hundred years. Communications systems play a larger role than ever in providing a tactical advantage to those forces that are network enabled, sharing synchronized situation awareness, and conducting network-centric operations. While the U.S. Military is no longer the dominant player in the global advanced communications technology market, it is still an important consumer. This market position and the high cost and risk of being on the “bleeding edge” of communications technology is driving the U.S. Military toward a new acquisition strategy that focuses on the rapid integration and fielding of state-of-the-shelf commercial products based communications systems to its globally deployed forces. Lessons learned from many years of experimentation and from recent combat operations in Afghanistan and Iraq clearly support the

importance of networking the force and making major improvements in communications systems. Key priorities for future modernization include: putting flexible communications and robust situational awareness capabilities within reach of every soldier; providing extremely robust, high capacity, multi-media on-the-move communications; self-forming, self-healing mobile networks; full ISR integration in C4 networks; robust urban and underground communications; and multi-function RF systems.

References:

Arthur K. Cebrowski and John J. Garstka, *Network-Centric Warfare: Its Origin and Future*, Proceedings, January 1998.

Charles Dervarics, *Seeing Blue: Blue Force Tracking*, C4ISR Journal, Oct 2005, pp. 42-46.

Terry Edwards, *Linking the 3rd Infantry Division (3ID) Into the Joint Network Node (JNN)*, Army AL&T Magazine, July-August 2005, pp.4-9.

Stephen Fox, *JSTARS Adds Blue Force Tracking Capability*, U.S. Air Force Press Release, Electronic Systems Center Public Affairs, Hanscom Air Force Base, January 19 2006.

Jeff Hawk, *Mobility-Hungry Army Awaits Wireless Upgrades*, Signal, Sep 2005, pp. 53-56.

Maryann Lawlor, *War Validates Netcentricity Concept*, Signal, Nov 2005, pp.17-22.

Frank Tiboni, *Army Successfully Tests WIN-T*, Federal Computer Week, December 2005.

U.S. Department of Defense Directive 8100.1, *Global Information Grid (GIG) Overarching Policy*, 19 September, 2002.

U.S. General Accounting Office Report GAO-04-858, *The Global Information Grid and Challenges Facing Its Implementation*, July 2004.

Nancy J. Wesensten, Gregory Belenky, and Thomas J. Balkin, *Cognitive Readiness in Network-Centric Operations*, Parameters, Spring 2005, pp. 94-105.