

USAWC STRATEGY RESEARCH PROJECT

CONVERGING THE NETWORKS

by

Lieutenant Colonel Leith A. Benedict
United States Army

Captain Donald Root
Project Adviser

This SRP is submitted in partial fulfillment of the requirements of the Master of Strategic Studies Degree. The U.S. Army War College is accredited by the Commission on Higher Education of the Middle States Association of Colleges and Schools, 3624 Market Street, Philadelphia, PA 19104, (215) 662-5606. The Commission on Higher Education is an institutional accrediting agency recognized by the U.S. Secretary of Education and the Council for Higher Education Accreditation.

The views expressed in this student academic research paper are those of the author and do not reflect the official policy or position of the Department of the Army, Department of Defense, or the U.S. Government.

U.S. Army War College
CARLISLE BARRACKS, PENNSYLVANIA 17013

Report Documentation Page			Form Approved OMB No. 0704-0188		
Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.					
1. REPORT DATE 30 MAR 2007	2. REPORT TYPE Strategy Research Project	3. DATES COVERED 00-00-2006 to 00-00-2007			
4. TITLE AND SUBTITLE Converging the Networks		5a. CONTRACT NUMBER			
		5b. GRANT NUMBER			
		5c. PROGRAM ELEMENT NUMBER			
6. AUTHOR(S) Leith Benedict		5d. PROJECT NUMBER			
		5e. TASK NUMBER			
		5f. WORK UNIT NUMBER			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) U.S. Army War College, Carlisle Barracks, Carlisle, PA, 17013-5050		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					
14. ABSTRACT See attached.					
15. SUBJECT TERMS					
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT Same as Report (SAR)	18. NUMBER OF PAGES 21	19a. NAME OF RESPONSIBLE PERSON
a. REPORT unclassified	b. ABSTRACT unclassified	c. THIS PAGE unclassified			

ABSTRACT

AUTHOR: Lieutenant Colonel Leith A. Benedict

TITLE: Converging the Network

FORMAT: Strategy Research Project

DATE: 26 March 2007 WORD COUNT: 5896 PAGES: 21

KEY TERMS: Net-Centric Warfare, Joint Network Node (JNN), Warfighter Information Network Tactical (WIN-T)

CLASSIFICATION: Unclassified

Unprecedented technology infusions into the combat formations has provided tremendous capabilities but with unintended consequences to the Network. Because legacy communications equipment failed to provide the necessary bandwidth to support Warfighters requirements at the point of impact, Combat Support and Combat Service Support communities began procuring their own communications solutions. What resulted was the beginning of the “deregulation” of the network and the emergence of a federation of stove piped, non-interoperable communications networks and systems.

Recent combat operations clearly demonstrated the considerable communications shortfalls at the tactical and operational level. To address the shortfalls, the Joint Network Node (JNN) program was rapidly developed and fielded. JNN's innovative design integrates state of the art commercial and governmental off the shelf technologies which provide more capability than any previous generation system.

JNN will mitigate the current bandwidth shortfalls at the tactical and operational level. In addition, further improvements can be accomplished by redesigning the network architecture to eliminate duplicative networks and migrate selected federation networks into a single, common architecture. Which leads to the question, should these stove pipe systems be migrated into the common user transport architecture?

CONVERGING THE NETWORKS

The time to fix bandwidth problems is now, before we deploy to the next fight¹

—Gen William S. Wallace

In order to fully realize and capitalize on the power of the “Network” enabled force and the benefits of Net-Centric Warfare, the Army must address three significant communications challenges: the looming bandwidth issue, integration of the disparate communications networks, and redesigning the technical architecture for the future forces. All three of these issues will become paramount for success of the Future Combat System (FCS) 1+1+14, consisting of the Soldier, the Network and the 14 networked platforms. First and foremost will be equipping the Soldier with the most advance technology available, but what will prove to be the greatest challenge will be integrating and synchronizing the vast array of sensors, platforms, and communications systems into a seamless, interoperable Network.

Operation Iraqi Freedom provided a glimpse into the future of warfare; agile forces executing full spectrum warfare enabled by state of the art technology. The military’s dependence on advanced, information technologies was clearly evident during the V Corps drive to Baghdad, Iraq and many have pointed out that the unprecedented twenty one day operation validated the new way of war, Rapid Decisive Operations, as it quickly overwhelmed Iraqi defenses. This new concept of warfare characterized by increased lethality, mobility, dispersed forces, increased operational tempo, and simultaneous actions across a non-linear battlefield kept the enemy off balance and devastated their decision cycle.

The recent combat operations also unmistakably demonstrated the inadequacy of our current generation of tactical communication systems and the significant communication bandwidth shortfalls that exists between the operation and tactical forces. Command posts established in fixed facilities, where both bandwidth and connectivity were not significant problems, had near real time Situational Awareness (SA) which provided an unprecedented view of the battlefield. This fused blue and red picture displayed the location of coalition forces and engagements but most importantly how the enemy forces were arrayed. This was not the case at the pointed end of the spear where combat is won or lost; brigade and below.

Data requirements supporting combat operations have increased almost exponentially in comparison to the bandwidth available, placing an enormous challenge on the archaic generations of communications equipment currently in the field. The data explosion of the late 1990’s radically transformed how the Army fought, leading to the transition from a voice centric, acetate map based force to a digitized force dependent on multiple data feeds in order to

provide a common understanding of the battlefield. Imagery, file sharing, e-mail, collaborative tools and tactical Video Teleconferencing (VTC) replaced the telephone and tactical fax machine as the primary means of communications. Proliferation of sophisticated, complex computer networks' at all command levels, each providing unprecedented access to vast amounts of data in which to prosecute combat operations.

Over time, technological insertions and upgrades to the communications systems improved data capabilities at the operational and tactical level but this effort couldn't keep up with the ever increasing bandwidth requirements. Forces deployed in austere environments required access to data services similar to capabilities provided in garrison. Existing limitations of the legacy communications systems coupled with the inability of the Signal Corps and the Acquisition community to stay in front of the data bow wave and provide solutions, caused Warfighters to look elsewhere to solve their bandwidth shortfalls. This was the beginning of the "deregulation" of the network from the grasp of the signal community and what has been described as a "free-for-all" in communication systems procurements. Systems were procured without regard to a technical architecture, resulting in a federation of stove-piped communications systems and networks that are operated outside the common user architecture.

The intent of this SRP is to examine what efficiencies can be gained by converging these disparate networks into a single, seamless common user architecture that can meet the bandwidth requirements of all users, ultimately pondering the question, is the time right to force the migration of these community owned, stove pipe systems into a common user transport architecture and eliminate the duplication of efforts.

Shortfalls of the Area Common User Legacy Systems (ACUS)

The primary shortfall of the current legacy communications systems is the bandwidth available to transport data communications. Bandwidth is the life blood of any communications network and measures the rate or capacity that data moves from one electronic device to another, usually expressed in bits per second.² In the tactical environment the typical data rates supporting deployed command posts ranges between 256 to 2048 Kbps. These data rates are somewhat misleading, although they appear to provide considerable capacity, 93% of the bandwidth is dedicated to voice channels leaving only 7% available to transport data.³ (Discounting recent initiatives to increase data capabilities within the MSE network associated with the Bridge to Future Networks efforts.)

Mobile Subscriber Equipment (MSE) was the flagship communications system for the Army. Designed and approved in 1979 as a non-developmental item (NDI) program, it was rapidly fielded starting in 1988 and was completely fielded throughout the Army by 1993. The original design did not include a data capability since computer network protocols had not matured sufficiently enough to be integrated into combat systems. Although MSE was capable of interfacing with tactical satellite such as GMF, it was primarily a terrestrial Line-Of-Sight (LOS) system. Cutting edge at the time, it provided secure voice communications to both fixed command post locations and limited mobile voice communications as you transitioned through the set grid network.

MSE was suitable for a linear battlefield with the doctrinal deployment of a corps with five divisions on line, each deploying their node centers to establish the grid network within LOS distances, GMF terminals providing doctrinal connectivity between higher and lower headquarters as well as reach-back connectivity into strategic networks. Within the MSE grid network you had an environment of the “haves” and “have nots” because of the number of command posts that the signal battalions had assets to support. Support was provided down to brigade and Combat Support (CS) and Combat Service Support (CSS) battalion command posts but not normally to maneuver battalion command posts. For the maneuver battalions, the primary means of voice communications was provided by FM radio and augmented with mobile secure remote terminals. Common Operational Picture (COP) was provided through additional systems such as FBCB2 Enhanced Position Location Reporting System (EPLRS) or Blue Force Tracker (BFT) but these are not collaborative tools suitable for sharing large, several megabit data files. FBCB2-EPLRS is a LOS system that requires a network of systems in order to maintain connectivity whereas BFT is an L-band space based satellite system.⁴

The two major shortcomings of the MSE system were network installation timeliness and the inability to provide data communications while on the move. In order to maintain reliable communications, the backbone of the grid network needed to remain static. Moving nodes was time consuming and while the node is in the process of moving it could not provide communications services until it was reestablished into the grid network. Reinstallation of the node center required four hours to establish the radio links and bring the switch on line. Because of these limitations, MSE was not well suited to support rapid operations with extended lines of communication and formations constantly on the move. Additionally, in order to benefit from the data communications that MSE provided, you had to be physically connected (hardwired) into one of the nodes since the system could not provide wireless data on the move.

These shortcomings were apparent during V Corps movement north to Baghdad during OIF, where division and brigade formations frequently outran communications coverage requiring the formation to stop and conduct a “tactical pause.” These pauses were a result of the overwhelming tactical success outpacing the archaic communications systems and required the formations to stop to re-establish communications in order to get updated, critical battlefield situational awareness; “where am I”, “where are my buddies”, and most importantly “where is the enemy?” Installation of the grid network within Iraq was challenging due to the pace of the operation, dispersion of forces, and because the search for WMD did not afford time to establish the full network.⁵ Node centers established point to point networks or hub-spoke connectivity with the network located in Kuwait, providing “wide band belts” along the invasion route in order to provide critical updates, but frequently the operational tempo at lower echelons did not provide the time necessary to install the full network.⁶

In testimony before the Subcommittee on Terrorism, Unconventional threats and Capabilities Armed Services Committee in October 21, 2003, General William Wallace, V Corps commander, highlighted the “digital divide” that exists within the current force. Most notably the fact that within the within the Army Corps (III, V and XVIII) there is no standardization in the digitization efforts, with III Corps fully digitized and networked while the other corps because of funding limitations and programmatic decisions, were forced to develop their own C4I architectures that were diverse and incompatible.⁷

A good case and point was the Command and Control vehicle that General Wallace used during OIF. The communications capabilities integrated in his command and control vehicle provided an unparalleled view of the both the battle space and blue formations but this tremendous capability was not available to his subordinate commanders.⁸ Not having these same capabilities throughout all combat formations made synchronizing the battle space difficult. While his C2 vehicle could receive UAV downlinks and provide Battle Command on the Move, subordinate commanders were limited to voice communications, either FM or single channel tactical satellite, in order to develop situational awareness.

A key lesson learned from OIF pointed to the fact that MSE clearly wasn’t capable of supporting high tempo operations and as General Wallace stated in his testimony before the House Armed Services committee, “must be replaced as quickly as possible.”⁹

Task Force XXI Advance Warfighter Experiment

In 1993, recognizing the power of a networked force, the Army’s modernization efforts focused on “Digitizing the Force.” Primarily an effort to provide increased situational awareness

and common operational picture, it focused on providing near real time data on combat capabilities and dispositions of both enemy and friendly forces in a shared collaborative environment down to the individual fighting vehicle. The concept proved promising; improving the combat power of the formations through the use of the knowledge provided by newly developed hardware and software applications, validated the Task Force XXI Advance Warfighter Experiment concept. More importantly, it identified the shortfall was not the new applications and technology, but the limited bandwidth available within the ACUS network.

The Signal Corps, using experiences gained from the AWE and recognizing that future conflicts would require more robust data networks, developed a two pronged approach to address the bandwidth shortages within the current force. The first objective was the development and fielding of new data technology to replace the existing tactical packet network within the MSE network. Secondly, the Signal Corps began developing the requirements for the future command and control communications network, designed to capitalize on emerging technologies and anticipated future Warfighter requirements. In November 1999, the Warfighter Information Network – Tactical (WIN-T), Operational Requirements Document was approved and resulted in the multi-billion dollar WIN-T program.

WIN-T was designed to provide increased bandwidth for data communications and improved mobile capabilities supporting battle command on the move. Additionally, the design of the equipment would provide for quicker installation and displacement, enabling the system to rapidly provide full C4 capabilities in a high tempo environment, supporting new and emerging operational concepts such as communications at the “halt” and the “quick halt.”¹⁰

The principal challenges were how to rapidly design and field this expensive system in the funding environment that existed before GWOT and whether the cumbersome acquisition process, which many have lamented, is not responsive enough to truly capitalize on current and emerging technologies, could design, develop and field the system Army wide. To date, critics of the WIN-T acquisition process have been proven correct. After JROC approval in 2001, the initial operational capability (IOC) was set for 2008. In July 2006, IOC was slipped five years to 2013, leading many to wonder if WIN-T will be obsolete before it is ever fielded.¹¹

Documenting the Bandwidth Shortage

The Congressional Budget Office (CBO) conducted an extensive investigation into the Army’s bandwidth challenges as a result of the Task Force XXI AWE initiative. This study was a top-to-bottom look at all available communications means for voice and data currently used by forces during the prosecution of combat operations, to include Combat Arms (CA), Combat

Support (CS) and Combat Service Support (CSS) organizations. In 2003 the CBO published their report summarizing the critical review of the bandwidth at the various command levels titled “Army Bandwidth Bottleneck.” This report detailed the communications capabilities by echelon and identified the expected data rates available with the ACUS network listed in the figure 1 below.¹²

Command Level	Bandwidth Supply	Peak Demand	Relative Supply Versus Peak
Corps	2550	3000 – 10000	1: 1 to 4
Division	533	2500 – 4000	1: 5 to 8
Brigade (corps)	533	800 – 1300	1: 1.5 to 3
Brigade (below)	37	800 – 1300	1: 20 to 30
Battalion	37	500 – 750	1: 10 to 20
Company	15	30 – 100	1: 2 to 6
Platoon	15	10 – 30	1: 0.5 to 2
Squad/veh	1.7	3 – 10	1: 2 to 6

In Kilobits per second

Congressional Budget Office

Figure 1.

Key points identified by the study can be summarized in three distinct categories; bandwidth available, measured peak demand, and the corresponding shortage during peak demands. From the peripheral, it would appear that higher echelons of command had suitable and dependable bandwidth available. When comparing available bandwidth with the peak demand, normally associated with planning or executing a major operation, the measured demand was four times the available bandwidth. This is further exasperated at lower echelons where the available bandwidth is considerably less. Most noticeable was disparity between brigade and battalion, where the bandwidth throughput was a dismal 37 Kbps - the critical points at which kinetic operations are executed have the least available bandwidth.

The disparateness in the communications capabilities between the echelons couldn't be addressed in the immediate term with modernization efforts or technology inserts and many

point to this as the reason that organizations began procuring transport systems to increase bandwidth and capabilities.

The Federation of Networks

The technological improvements over the past decade have significantly impacted how the Army operates. Enhanced capabilities, to include the maturation of the battlefield operating systems, combined with significant advances in software applications and the increased density of hardware systems, have placed considerable demands on the Network. Regardless of the location on the battlefield or type of headquarters, the Army has become dependent on robust data networks in order to operate. Numerous manual business processes now are completely automated resulting in unprecedented efficiencies but these improvements came at a cost.

The deployable infrastructure supporting this revolution failed to keep pace. Several military communities couldn't wait for WIN-T or 2013; they needed robust bandwidth at deployed locations now, especially in light of the pace of the deployments for the Global War on Terrorism. Most notably the intelligence and the logistics communities chose to procure their own communication transport systems to meet their requirements. Pandora's Box was open; if you could afford the communications system and agree to operate it at your own expense, you could get into the transport business. These types of procurements are a major challenge to maintaining viable network architectures and guaranteeing interoperability. Since these procurements sought to only meet the individual community's needs, very little thought was given to developing a solution that would benefit the common user community resulting in disparate, distinct network architectures operated outside the operational sphere of the Signal Corps.

Trojan Spirit

Addressing their unique requirement for Top Secret data during Desert Shield/Desert Storm, the Military Intelligence community designed and fielded the system known as Trojan Spirit II Communications Central. The system was rapidly fielded in the early 1990's, providing cutting edge technology before computer networks were common place in the tactical environment. This innovative design addressed a critical shortfall that MSE could not provide since MSE was only accredited for secret level traffic. During this time the only Top Secret circuitry was provided through the AN/TYC-39 message switch, which provided hard copy record traffic. The communications central is an intelligence dissemination satellite terminal and the center of the MI Special Compartmented Intelligence (SCI) and collateral network

architectures, providing strategic reach-back connectivity, integrating intelligence communities at all levels, strategic to tactical.

Trojan Spirit II is a deployable Tri-band satellite terminal capable of providing Top Secret and Secret data at bandwidths varying from 4.8 to 512Kbps and provides local and wide area network connectivity as well as limited TS phone services.¹³ Another key aspect of the Trojan network is the unique network architecture that provides a global point of presence through twenty-seven fixed locations that can provide services in every Combatant Commanders Area of Responsibility.¹⁴ The architecture includes centralized network management functions to include technical support, network monitoring and network defense.

Trojan Spirit can be viewed as one of the first rapidly fielded communication system that bypassed the normal, cumbersome developmental and acquisition cycle. Taking readily available, proven commercial technology and utilizing commercial industry standards instead of proprietary protocols, Trojan Spirit can interface with numerous signal C4 systems at the network level and provide significant routing/transmission alternatives if integrated into the common user architecture. A significant drawback to integrating the Trojan Spirit into the common user network is that when deployed, it is normally physically located within high security areas supporting the military intelligence enclave.

In 2001, the commanding generals of both the Military Intelligence Center and Signal Center both approved the Trojan Spirit to Warfighter Information Network migration plan that would move the Trojan Spirit (capabilities and network support) to the Signal community under TSM – Satellite Communications.¹⁵ Although the migration was agreed to, this effort has not been accomplished, and reviewing current and future Trojan Spirit funding in the Army Budget, it is unlikely that this will be accomplished in the near future.

Combat Service Support Very Small Aperture Terminals CSS-VSAT

The logistic community has also developed numerous sophisticated web based tools for automating logistics functions. These new tools provide near real time visibility on the status of requisitions, throughout the wholesale and distribution systems, in response to the challenge of providing in-transit visibility. However, these new tools require more bandwidth than what ACUS could provide and when coupled with how the logistics community typically deploys, geographically dispersing their logistics activities, compelled the logistics community to search for a solution. The Army G4 sponsored solution was the Combat Service Support Very Small Aperture Terminals or CSS VSAT, a 1.2 meter dish, transit cased satellite system that is rapidly deployable and capable of providing network communications for the near real time status of

requisitions and reports with DoD logistical activities and the civilian industrial base.¹⁶ Most of the customers that the Army logistical units interface with do not have access to classified networks and as a result, the majority of their business transactions are conducted using the unclassified internet. CSS-VSAT fulfills their unclassified requirements by providing wide-band NIPRNET reach-back access and has world wide coverage through one of the four teleport locations strategically located around the world. The primary drawback to CSS-VSAT is that it only benefits the logistical community, providing a separate, distinct network that does not complement the common user network. Like the Trojan Spirit network, CSS-VSAT is supported by a 24/7 network support center that provides technical support, network monitoring and network defense.

Both of these are examples of networks that are outside the purview of the traditional architecture and challenge a centrally managed network architecture and impede the transition to a seamless Network. Both of these solutions depend completely on satellite bandwidth and do not have an alternate capability, such as line of sight, which will be significant if deployed to austere locations where commercial and military satellite coverage is constrained. These systems will have to compete with command and control communications priorities for satellite bandwidth, putting the functionality of these systems at risk.

Addressing Shortfalls

Realizing that WIN-T's benefits would not be realized during the current conflict and when combined with the lessons learned during Operation Iraqi Freedom, USCENTCOM submitted an Urgent Needs Statement identifying the immediate need for an improved, deployable communications system complete with a supporting architecture. The Signal and Acquisition community clearly understood the need to provide an interim capability to the Warfighter and developed the "Bridge to Future Networks" concept which in conjunction with the road map to WIN-T, would spin out improved interim capabilities and provide funding for continued upgrades to the existing legacy equipment throughout the force (Active, Reserves and National Guard)¹⁷.

A significant spin out was the Joint Network Node (JNN) program, a quantum leap in capability and technology, and the first communications system specifically designed for Internet Protocol (IP) communications. JNN is an integrated state of the art commercial and governmental of the shelf information technologies capable of providing voice, video and data in self-contained, deployable packages capable of providing 119 Mbps of internet based connectivity to each divisional footprint.¹⁸ Major components consist of the hub terminal, joint network node, and the battalion command post node. The architecture is designed to directly

support the modularized Brigade Combat Teams (BCT's) with organic reach-back capabilities to the Global Information Grid (GIG) for DISN services (NIPRNET, SIPRNET, voice and VTC). Most importantly users, at the battalion level and below, now have access to sufficient bandwidth more than capable of supporting operations without procuring additional communications systems such as the CSS VSAT or Trojan Spirit.

JNN's innovative design uses technology based on industry standards, instead of proprietary protocols, and the equipment is similar to what is used in most commercial networks. It provides data trunk switching, telephone, local and wide area networks, reliable network management, and services regardless of the environment. An advantage that JNN offers over previous generations of communications assemblages is that after the kinetic phase of the operation is over and stability operations begin, the equipment within the JNN node can be dismounted and installed into hardened structures to form the core of the strategic network, Technical Control Facility (TCF) supporting the forward deployed location. With the addition of commercial satellite systems such as the DKET and using contractors to operate the TCF, the soldiers can be released to redeploy and the JNN assemblages can be retrofitted with replacement equipment as a part of the equipment reset, rapidly prepared for future operations.

JNN spirals 1-7 (BCT's and Echelons above Corps Signal Battalions) have been procured and fielded using supplemental funding but future procurements have hit a significant roadblock. Congress has expressed concern over the JNN program for two primary reasons. First, JNN's rapid development in response to an urgent needs statement was met by integrating COTS/GOTS equipment using a sole source contract and not competitively bid, coupled with the fact that JNN is not a joint system, or an official system of record.¹⁹ Secondly, the appearance that JNN and WIN-T appear to be duplicative programs and the Army has not fully developed the plan to access how best to transition from JNN to WIN-T.²⁰ Congress has mandated that fielding of additional JNN sets be put on hold and have held up the funding until the Army addresses their objections. This leaves the Army leadership with two options; develop JNN into a program of record to include the milestone process and competitively bid the program, which will increase the cost and add years to the acquisition, or restructure the WIN-T program and integrate JNN into the WIN-T program.²¹ Both solutions require JNN to complete OPTEC certification.

Migration Challenges

The Army budget provides some insight into how significant bandwidth and the Network have become, yet also identifies how decentralized the communications equipment

procurement has become. In the 2006/2007 Army budget, under the Other Procurement Army Communications and Electronic Equipment section, illustrate 61 programs of record with expenditures in the billions in both hardware and software, which are impacted by the Network.²² Of the 61 systems only six expand the capacity of the tactical network, primarily space and terrestrial communications. The remaining programs are enablers that will improve the Army's lethality but all have a common denominator, they require the Network in order to produce the desired effects. Funding for these enablers and the future network are not synchronized with applications and hardware being delivered before the supporting network capacity will be available. Frequently, applications are independently developed in a sterile, bandwidth unconstrained environment which when integrated into the network, are challenged to operate in the congested environment.

Communities procuring stove piped satellite transport systems compete directly with the common transport architecture provided by JNN and eventually WIN-T for critical resources beyond just the budget. Recent estimates of satellite transponder usage supporting both Operation Enduring Freedom and Operation Iraqi Freedom show that 80 percent of the bandwidth supporting stability and support operations in the CENTCOM AOR is being provided by commercial satellite providers.²³ This is a direct result of the proliferation of satellite transport systems which overwhelmed the military satellite capacity in the region. Radio Frequency (RF) spectrum, both space based and terrestrial, is not an infinite resource. Migrating and integrating these assets into the common user network would increase the bandwidth available, reduce satellite costs by eliminating redundant satellite links or links that have low usage rates, and assist in optimizing the common user network architecture.

Because of the methodology used in fielding both Trojan Spirit and CSS-VSAT, critical acquisition processes were bypassed, including the essential linkages to the acquisition pillars of Doctrine, Organization, Training, Material, Leadership, Education, Personnel and Facilities (DOTMLPF). This presents a considerable problem since the cradle-to-grave lifecycle management for these solutions was not integrated into a comprehensive fielding package. Two easily identified significant shortfalls were in the organization and training pillars. The systems did not include Signal Soldiers to operate the assemblages, resulting in non Signal Soldiers operating the equipment from within the organization. Military Occupational Skills not related to the communications field were assigned to Install, Operate and Maintain (IOM) these complex systems. Secondly, the operator training consisted of learning the basics, how to install the satellite system, locate the satellite and connect the network interface devices but comprehensive training on satellite theory, network topology and extensive troubleshooting was

not included in the package, cementing an extensive dependence on contractors to keep the system fully operational.

The migration of these systems into the Signal Corps domain will require a reassessment across the DOTMPLF to ensure that the systems are supportable over the long term but the Signal Corps has an satellite operator -maintainer MOS that could be expanded to include these satellite systems. The personnel cost savings will not provide a significant saving but having MOS trained operators operate these assemblages will improve systems reliability and the Network.

With the fielding of Joint Network Node and improved capabilities at the lower organizational levels provided by the battalion command post node, are these other networks necessary? This question is best answered by analyzing the information-exchange requirements and specific network domains that organizations such as the logistics or intelligence communities need to operate in. Capabilities wise, JNN can provide sufficient bandwidth and services (DISN, SIPR, NIPR and JWIC's with appropriate encryption devices) to meet most of the documented requirements. Both Trojan Spirit and CSS-VSAT have reoccurring operational costs when in operation which could be reduced by using services provided by the JNN network.

This is not to say that JNN will fix everything, but integrating Trojan Spirit and CSS-VSAT into the JNN network under signal control, where the resident network expertise can best design and integrate the network architecture, will benefit the entire community.

Command and Control of the Network

As the military moves towards Net-Centric warfare, centralized command and control of the network has become more essential to managing the complex network architecture, a hybrid network consisting of strategic, operational and tactical communications. Decentralizing the management of any network is a recipe for disaster, since it presents numerous seams that can be exploited or lead to significant network outages since no single organization is in charge of the health, maintenance and restoration of the Network. The Army's concept of NETOPS provides for improved defense in depth and collaboration between the tiered network control elements, the difficulty is clearly delineating the responsibilities across the numerous network domains in real time when a significant event has occurred within the Network. Clearly identifying ownership of links, segments and domains is critical in ensuring unity of effort in providing reliable communications services to deployed combat forces. Case and point for the hybrid network in Iraq, the primary responsibility for the integration and synchronization for all

communications requirements fall into the coalition, joint, corps, division, brigade and battalion “6” communities. These communities are responsible for the planning, employment, management and day to day health of the Network, and have the “on the ground” challenge of integrating the stove piped, disparate systems into coherent, useable network architectures.

Within Kuwait, the CFLCC Theater Network Operations Security Center has technical Control of the strategic theater network to include both Iraq and Afghanistan. Within Iraq, Multinational Corps Iraq (MNCI) C6 is primarily responsible for all C4 requirements within the country, to include service components and coalition partners. The day to operation of this vast network is the responsibility of the Coalition Network Operations Security Center (CNSOC). Within the CNOSC they use advanced network health and monitoring tools to proactively manage the numerous links and networks deployed throughout the country but they can only provide network oversight for the networks that they have operational control of.

Both the Trojan Spirit Network and CSS-VSAT are not under the operational control of the CNOSC, which poses several challenges since they connect to the larger network. Both Trojan Spirit and CSS-VSAT are supported by network support centers which reside outside of the theater and have field technicians in theater to assist in configuration, installation troubleshooting and network issues. But because their networks are not monitored by the CNOSC, when they are having network problems, the CNOSC or other in-theater Net-ops centers do not have the ability to analyze their outages to look for impacts within the theater architecture. Same is true when the network is under attack, the CNOSC has limited capabilities to look into the theater network to determine and correlate events and take appropriate action to minimize the impact to the network but the technicians within the CNOSC have no ability to provide assistance to segments of the architecture that are outside their control.

The Combat Service Support Automation Management Office (CSSAMO) is responsible for the management of the automation equipment and networks supporting the logistical community. Within this organization you have some resident expertise in system administration, local and wide area networks administration and expertise in logistical applications but they are not transmission experts, they are not the same as telecommunications engineers and have virtually no experience in planning or managing large networks. One of the key logistical lessons learned from Operational Iraqi Freedom as reported in the Center for Army Lessons Learned, concerned their ability to manage Standard Army Management Information Systems VSAT Satellite Network in OIF stated: “CSSAMO and battalion personnel are not properly trained to manage MSE NIPRNET and VSAT NIPRNET systems.”²⁴ This validates the point that deregulating the procurement of communications systems and the management/control of the

network to organizations that are neither trained nor equipped to perform critical network operational functions is detrimental to providing the seamless, integrated network required to ensure information superiority and Net-Centric operations.

Technical Architecture

The Army CIO/G6 is the proponent for Army's technical architecture for tactical communications and is responsible for providing guidance, standards, policy, procurement strategies, synchronizing capabilities with requirements, and developmental oversight of the technical architecture supporting the network. Previously, the technical architecture served as the road map for the systems procurement, ensuring interoperability and compliance while providing common user communications as a part of an overarching strategy. Because the architecture and the equipment supporting it failed to keep pace with requirements, the result was the deregulation of the network and unparalleled, frenzied procurement of transport systems by CS and CSS organizations. The technical architecture today can best be described as a kluge of stove piped transport systems, disparate networks, disjointed network operations, and segmented command and control, not a seamless, interoperable, self healing network necessary to conduct Rapid Decisive Operations much less what will be required to support the Future Combat System.

The recently published Network Centric Warfare Case Study, conducted by the Center for Strategic Leadership, identified 35 separate distinct C4ISR architectures within the Department of Defense, all with considerable ramifications on the Network.²⁵ A majority of these architectures are stove piped systems and are not interoperable. In some cases, the new architectures were a result of recent fielding initiatives by the acquisition community and the design of equipment included a new network architecture, designed outside of the common user architecture.

Because the Network is not homogenous and horizontally integrated, every step forward taken has resulted in two steps backwards. This is because of the fact that we are not procuring systems towards a common architectural goal and are frequently forced to develop expensive, backwards compatible or "gender bender" solutions in order to integrate technology to overcome stove piped systems.

Conclusion

Recognizing that the signal community had "lost sight of the Network" the CIO/G6 is now reasserting "responsibility" for the network and attempting to move towards a single enterprise network²⁶. Recent briefings by the CIO/G6 include the Joint Network Transport Capability Spiral

(JNTC-S) initiative which as briefed includes both “connect the logistician” with CSS-VSAT (an Army G4 initiative not CIO/G6)²⁷ and Intel (Trojan Spirit) integrated into the technical architecture, as a part of the bridge to WIN-T. The briefings do not address how, or when, this will be accomplished; only “converging the Intel networks and CSS networks must continue.”²⁸ This implies consensus within the CS and CSS communities, but a closer look at their current procurement strategies proves this doesn’t seem to be the case. Herein lays the challenge; JNTC-S can be seen as a re-engineering effort to reassert control of the architecture, but what are the incentives or mechanisms to force compliance? Since both of these systems are funded independently of CIO/G6 influence, forcing their migration into JNTC-S can only be accomplished with some form of leverage (budget or policy) which forces compliance to the bridge to WIN-T architecture.

Whether these systems converge into the JNCT-S Network remains to be seen. It is not a question of technical feasibility, the integration of the equipment can be accomplished quickly, but the effort must move beyond briefing slides. An agreed upon migration plan, with transition milestones and compliance dates, must be developed if this initiative is going to be successful.

The new efforts by the Signal community to reassert “ownership” of the Network after years of neglect is an important first step in revamping the technical architecture and migrating existing communications networks to better support Warfighter C4 requirements. The potential savings in terms of optimizing network bandwidth, realigning manpower, reducing communications procurement costs by eliminating duplicative efforts, and streamlining network C2, will more than pay for the initial costs for this endeavor. The largest challenge will be getting unanimous buy-in from all the Network stake owners.

Finally, CIO/G6 in concert with the Army Signal Center, must take the lead in developing, articulating and enforcing the technical architecture with the Program Managers and the Acquisition Community. This is critical to ensure that future programs are in compliance with the key technical parameters necessary for a truly seamless, interoperable network that will enable Net-Centric Warfare and information superiority.

Endnotes

¹ LTG William S. Wallace, Commanding General, Combined Arms Center, U.S. Army Training and Doctrine Command, *C4I Interoperability: New Challenges in 21st Century Warfare: Statement before the Subcommittee on Terrorism, Unconventional Threats and Capabilities Armed Services Committee*, 108th Cong., 1st sess., 21 October 2003.

² Congressional Budget Office, *The Army's Bandwidth Bottleneck* (Washington D.C.: Congressional Budget Office, August 2003), 1: available from <http://www.cbo.gov/showdoc.cfm?index=4500&sequence=1>; Internet; accessed 20 December 2006

³ Kevin J. Cogan, and Raymond G. DeLucio, *Network Centric Warfare Case Study: Volume II* (Carlisle Barracks, Pennsylvania: U.S. Army War College, 2006), 21-22.

⁴ John B. Tisserand III, *Network Centric Warfare Case Study: Volume III* (Carlisle Barracks, Pennsylvania: U.S. Army War College, 2006), 44-45.

⁵ Kevin J. Cogan, and Raymond G. DeLucio, *Network Centric Warfare Case Study: Volume II* (Carlisle Barracks, Pennsylvania: U.S. Army War College, 2006), 28.

⁶ Gregory Fontenot, E.J. Degen, and David Tohn, *On Point: The United States Army in Operation Iraqi Freedom* (Fort Leavenworth, Kansas: Combat Studies Institute Press), 174-175.

⁷ Wallace.

⁸ Ibid.

⁹ Ibid.

¹⁰ U.S. Army, *Warfighter Information Network – Tactical (WIN-T): Operational Requirements Document (ORD)*, 5 November 1999; available from <http://www.fas.org/man/dod-101/sys/land/docs/WIN-T5NOV.htm>; Internet; accessed 17 December 2006.

¹¹ *Network Centric Warfare Case Study: Volume II*, 52

¹² CBO, 3.

¹³ GlobalSecurity.Org, "AN/TSQ-190 Trojan/Trojan Spirit II Communications Central," available from <http://www.globalsecurity.org/intell/systems/trojan.htm>; Internet; accessed 20 December 2006.

¹⁴ Ibid

¹⁵ TSM Update Winter 2001. "TSM-Satellite Communications Update," available from <http://www.gordon.army.mil/winter/winter%2001/tsmupdt.htm>; Internet; accessed 20 November 2006.

¹⁶ PEO EIS News, 1 April 2005, available from <http://www.eis.army.mil/dcats/n-05-04-01.html>; Internet; accessed 10 January 2007.

¹⁷ U.S. Army, Procurement Programs, *Committee Staff Procurement Backup Book: Fiscal Year (FY) 2006/2007 Budget Estimates: Other Procurement, Army Communications and Electronics: Budget Activity 2: Appropriation*. (Washington, D.C.: U.S. Army, February 2005); available from <http://www.asafm.army.mil/budget/fybm/fy06-07/pforms/opa2.pdf>; Internet; accessed 15 December 2006.

¹⁸ United States Army Acquisition Logistics and Technology Enterprise Systems and Services, *JNN-Networks Smart Charts* (Washington D.C.: U.S. Department of the Army, 23 February 2006), 3.

¹⁹ U.S. Congress. Senate, *National Defense Authorization Act for Fiscal year 2007*, S.R. 109-254, 109th Cong., 2nd sess., 2006, sec 111.

²⁰ U.S. Congress, *National Defense Authorization Act for Fiscal Year 2007: Bridge to Future Networks*, H.R. 109-452 ,109th Cong., 2nd sess., 2006.

²¹ Network Centric Warfare Case Study Volume II, 55.

²² U.S. Army, Procurement Programs, *Committee Staff Procurement Backup Book: Fiscal Year (FY) 2006/2007 Budget Estimates: Other Procurement, Army Communications and Electronics: Budget Activity 2: Appropriation*. (Washington, D.C.: U.S. Army, February 2005); available from <http://www.asafm.army.mil/budget/fybm/fy06-07/pforms/opa2.pdf>; Internet; accessed 15 December 2006.

²³ LTG Steven W. Boutelle, "Army communications: Building Strong Networks for our Warfighters," *Army* (October 2006): 210.

²⁴ Center for Army Lessons Learned, *Operation Iraqi Freedom (OIF) CAAT II Initial Impression Report (IIR)* (Fort Leavenworth: Center for Army Lessons Learned, May 2004); available from http://www.globalsecurity.org/military/library/report/call/call_04-13.pdf; accessed 20 December 2006.

²⁵ *Network Centric Warfare Case Study: Volume II*, 58.

²⁶ MG Conrad Ponder, "Joint Network Transport Capability – Spiral (JNTC-S)", briefing to AUSA 13th Annual Space and Missile Defense Symposium, briefing slides with scripted commentary

²⁷ Stephen Larson, "Combat Support Connection," *Military Information Technology*, June 2005 [journal on-line]; available from <http://www.military-information-technology.com/article.cfm/DocID=993>; Internet; accessed 10 December 2006.

²⁸ Ponder

