

ARMY COMMUNICATOR

Approved for public release;
distribution is unlimited.
Headquarters,
Department of the Army

Voice of the Signal Regiment

PB 11-16-1 2016 Vol. 41 No. 1



COMMAND

Chief of Signal
BG Thomas A. Pugh

Regimental Chief Warrant Officer
CW5 Peter T. Winter

Regimental Command Sergeant Major
CSM Robert A. Daniel

EDITORIAL STAFF

Editor-in-Chief Larry Edmond

Art Director/Graphic Designer
Billy Cheney

Photography
Billy Cheney, Amy Walker, CPT Lisa Beum, 1LT
Jeremiah J. Snyder, SGT Kimberly Hackbarth

By Order of the Secretary of the Army

Patrick J. Murphy
General, United States Army
Chief of Staff

Official:

GERALD B. O'KEEFE
Administrative Assistant to the
Secretary of the Army

Authorization 1608901

Army Communicator (ISSN 0362-5745) (USPS 305-470) is published quarterly by the U.S. Army Signal School at Signal Towers (Building 29808), Room 713 Fort Gordon, Ga. 30905-5301. Periodicals postage paid by Department of the Army (DOD 314) at Augusta, Ga. 30901 and additional mailing offices.

POSTMASTER: Send address changes to *Army Communicator*, U.S. Army Signal School, Signal Towers (Building 29808), Room 713, Fort Gordon, Ga. 30905-5301.

OFFICIAL DISTRIBUTION: *Army Communicator* is available to all Signal and Signal-related units, including staff agencies and service schools. Written requests for the magazine should be submitted to Editor, *Army Communicator*, U.S. Army Signal School, Signal Towers (Building 29808), Room 713, Fort Gordon, Ga. 30905-5301.

This publication presents professional information, but the views expressed herein are those of the authors, not the Department of Defense or its elements. The content does not necessarily reflect the official U.S. Army position and does not change or supersede any information in other official U.S. Army publications. Use of news items constitutes neither affirmation of their accuracy nor product endorsement.

Army Communicator reserves the right to edit material.

CORRESPONDENCE: Address all correspondence to *Army Communicator*, U.S. Army Signal School, Signal Towers (Building 29808), Room 713, Fort Gordon, Ga. 30905-5301. Telephone DSN 780-7204 or commercial (706) 791-7204. Fax number (706) 791-3917.

Unless otherwise stated, material does not represent official policy, thinking, or endorsement by an agency of the U.S. Army. This publication contains no advertising. U.S. Government Printing Office: 1984-746-045/1429-S.

Army Communicator is not a copyrighted publication. Individual author's copyrights can be protected by special arrangement. Acceptance by *Army Communicator* conveys the right for subsequent reproduction and use of published material. Credit should be given to *Army Communicator*.

ARMY COMMUNICATOR

Voice of the Signal Regiment

Features

- 3 **Speaking with One Voice**
CPT Kyle D. Barrett
- 8 **Implementing Policies Electronically**
CPT Trenin D. Spencer
SFC Christopher L. Donald
SPC Ashley M. Ardiana
- 14 **Transition for WIN-T INC 1B to INC 2**
LTC P. K. Sayles
MAJ Daniel J. Kull
- 19 **Flying Command Post Global Response Exercise**
Amy Walker
- 24 **Signal Support to Infantry Combat Teams**
CPT Vernon Pittman
- 30 **Answers to the Test Lessons and Best Practices**
 Scott Gorectke
- 32 **Installation as a Docking Station**
Scott Gorectke
LTC Chris Wells
- 34 **Supporting a Strong Europe McArthur's Own**
LTC Delton Nix, Jr.
CSM Woody Carter
- 36 **2nd Signal Battalion Facilitating NATO Command and Control**
LTC John C. Hinkel, Jr.
- 40 **Tactical Mission Command in a Robust Multi-National Operating Environment**
1LT Jeremiah J. Snyder
- 44 **Team Building in the U. S. Army**
MAJ Cheryl L. Gray
- 46 **Supporting Mission Command for Pacific Pathways Malaysia**
CPT John Geracitano
- 49 **The Broken Interoperability Link**
CPT Brittany Coughran
- 54 **Mission Command Systems Integration in a Decisive Action Training Environment**
 CPT Julie A. Leggett

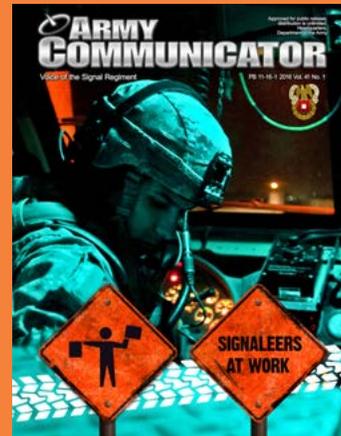
Join the Discussion

At the end of articles where you see this icon,  you can weigh in and comment on-line.

~On the Cover~

Signaleers at Work

U.S. Army SPC Tom Tienda tests the communications system of his armored vehicle before leaving Camp Taji, Iraq, SPC Tienda is a military policeman assigned to the 82nd Airborne Division's 2nd Brigade, Company H, 2nd Brigade Special Troops Battalion and one of the many who depend on the work of Signal Soldiers. Throughout this issue you will find pictorials of Signal professionals working in a variety of settings.



Cover design by Billy Cheney

Speaking with One Voice

The Network Modernization Roadmap illustrates our Army leaders' strategy to fill capability gaps and make necessary improvements to network functionality that ensures American Soldiers remain the most lethal fighting force on the battlefield.

By Kyle D. Barrett

Let's look at how we get to the future from where we are.

Today, the U.S. Army has tactical networks that connect commanders and Soldiers with voice and data capabilities to the lowest echelon.

However, the tactical network is pieced together with a myriad of mismatched systems that work well separately but were not designed to work together, requiring significant integration and configuration efforts. This “borne-of-necessity” approach has increased the number and size of communication platforms while introducing a great deal of complexity in how Soldiers interact with the network.

The Army’s tactical network of tomorrow provides robust communications that are rapidly deployable, versatile and scaled to fit a multitude of mission types. A recently published Army white paper titled Army Vision – Force 2025 describes future operations as “decentralized, distributed, and integrated.”

The Program Executive Officer for Command, Control, and Communications – Tactical has created a “Network Modernization Roadmap” that will guide the Army’s tactical network of today to a network capable of supporting operations in 2025. The roadmap consists of three phases that form building blocks: Network 2.0 from 2014 to 2016, Simplified Tactical Army Reliable Network from 2016 to 2020, and the Network after Next from 2020 and beyond.

The Army of 2025 is comprised of mission tailored units, organized with capabilities needed for a specific mission and environment, and are engaged regionally and deliberately across the globe. The Army has defined three lines of effort to optimize the force: force employment; science and technology and human performance optimization; and force design. The S&T line of effort concept is that technology drives concept,

meaning projected technological advancements serve as a template for future tactical communication concepts. While maneuver forces continue to refine their tactics and techniques on the battlefield, advances in S&T will allow maneuver elements to be even more agile and rapidly deployable. BG Daniel P. Hughes, program executive officer of PEO C3T “picture[s] a landscape in which Soldiers can start up a wireless command post at the push of a button, a quick voice command can summon and interpret a wealth of operational data, and a digital map looks the same from smartphone to tablet to vehicle-mounted touch screen.” Simplified tactical communication platforms that are lightweight and versatile, yet robust and secure, are essential to the successful evolution of Force 2025.

With Army Vision – Force 2025 as its guide, the Army Signal Corps and PEO C3T have begun to implement the Network Modernization Roadmap, which synchronizes the operational priorities of versatility, mobility and security with technology imperatives and program-of-record objectives. Over the last three years, the Army has fielded the Capability Set 14 network as an initial step toward network modernization. CS 14, also known as the Warfighter Information Network – Tactical Increment 2, introduces “on the move” satellite communication capabilities that allow company commanders and platoon leaders to stay situationally aware at all times, even when far away from their command post, thus empowering dismounted Soldiers with situational awareness through technical devices

and networking radios. More importantly, CPs can maintain accurate situational awareness in the dynamic decisive action environment. However, CS 14 has proven to be complicated and intimidating for some operators, primarily the commanders and leaders who operate the Soldier Network Extension and Point of Presence vehicle mounted platforms.

Recently Jennifer Zbozny, PEO C3T chief engineer, reported that a new simplified version of the SNE and PoP will be included with the next-generation network known as Network 2.0. While Network 2.0 includes a simplified user interface with communication platforms, the next-generation network provides commanders and network engineers with enhanced command and control capabilities.

With mission tailored, regionally aligned, and rapidly deployable units of Force 2025, rapid task organization for purpose is imperative. Network 2.0 includes technology where a commander may simply look at a battle command screen and drag-and-drop a unit icon to where it needs to go.

Task re-organization currently involves building a new mission plan and distributing it using a mission data loader – a task nearly impossible for units conducting continuous operations. Network management tools included in Network 2.0 are increasingly software based and share the same drag-and-drop simplicity when reconfiguring all nodes in a network. Simply put, Network 2.0 simplifies the human interface with network platforms while

(Continued on page 4)

(Continued from page 3)

bridging the Army's current technology and the lightweight and highly capable STARNet of 2020.

With communication security one of the top priorities of the Network Modernization Roadmap, and with cyber warfare on the forefront, increased use of radio transmissions are difficult. Challenges included in the STARNet is developing applications that use limited spectrum.

By 2020, advancements in waveform technology will allow operators to communicate while simultaneously jamming enemy signals-intelligence operations. STARnet's decreased physical equipment burden requires less power and decreases the overall footprint of future maneuver forces.

Currently, network management at the Brigade level requires 20 separate laptops and servers. As tactical communication platforms reduce their footprint, so do Network Operations

Centers. STARNet introduces the increased use of virtualization – through virtual local area networks and virtual private networks – and automated node management, decreasing the number of devices required for NetOps. Additionally, this network convergence effort will provide cloud computing so that strategic level echelons can take over some services once provided at the tactical level. This effort to decrease the size of NetOps Center corresponds with smaller brigade command posts of Force 2025.

The network is a key and essential part of the Army's vision of a leaner and more expedient force, able to adjust to any situation anywhere in the world. NaN, the final phase of the Modernization Roadmap, includes "adaptable solutions, to have our equipment adapt to different missions and challenges no matter where we are," says Zbozny of PEO C3T. Part of that adaptability will likely include a human-machine interface similar to Apple's Siri technology. With this technology, a

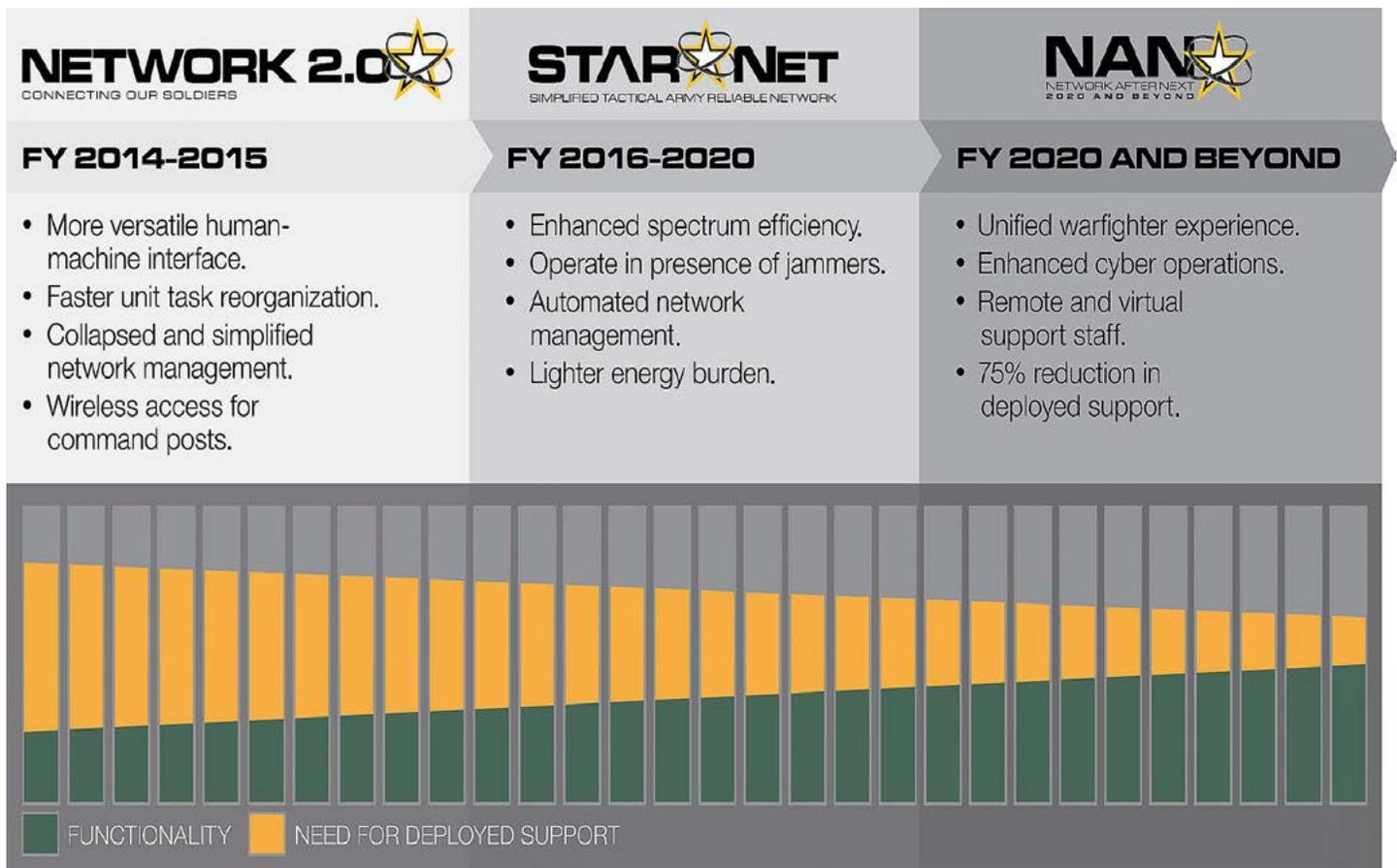


Figure 1

The U.S. Army Network Modernization Road Map synchronizes operational priorities for versatility, mobility and security with technology imperatives and program-of-record objectives. It comprises three interconnected phases: Network 2.0, STARNet and NaN.



The Warfighter Information Network-Tactical Increment 2 Point of Presence is the primary on-the-move configuration item to be installed on tactical combat platforms such as this Mine Resistant Ambush Protected All-Terrain Vehicle, at division, brigade and battalion echelons. It will be tested during the WIN-T Increment 2 Initial Operational Test and Evaluation scheduled for May at White Sands Missile Range, N.M.

“digital tactical butler” inside mission command systems aids commanders on the battlefield.

At lower echelons, the Army’s CS 14 delivers software-defined radios that communicate with smartphone-like technical devices. These technical devices are making mission objectives more transparent to higher commands through accurate position location information, text messaging, photo sharing, and full motion video feeds. The focus of the NaN is to “untether” the technical device from the radio, using Long Term Evolution, commonly known as 4G wireless technology, so that troops can communicate more seamlessly across echelons. A key component of NaN is the ability for data and voice transmissions to take a different “path” if an existing route has moved or is jammed. This seamless transition from radio to LTE to satellite, while difficult and complex is a critical element of the Network Modernization Roadmap and Force 2025.

PEO C3T and the Communications – Electronics Research, Development and Engineering Center have joined forces to develop a single tactical computing environment that will provide a seamless user experience from handheld devices to vehicle platforms to command posts. BG Hughes asks us to “picture a Soldier with multiple personal devices that all run an Apple, Android or Windows operating system.” Force 2025 operates in a tactical realm delivering “standard maps,

messaging, and icons that are intuitive to operate and reduce the training burden.” With respect to mission command, this standardized operating environment facilitates the Army’s transition from stand-alone mission command systems to an integrated warfighting system with user-friendly “widgets” or apps.

Further advancements in Joint Battle Command-Platforms enable inter-agency near-real-time mission command capabilities. The current Joint Capability Release Force XXI Battle Command Brigade and below evolves into the Joint Battle Command – Platform with the capability to communicate over a hybrid network--Soldier Radio Waveform and Satellite. Most importantly, the JBC-P is common to all branches of the military, allowing joint interoperability and unified mission command capabilities. The STARNet phase of the Network Modernization Roadmap, combined with the JBC-P, forms a multi-tiered joint communications infrastructure by 2020.

None of these advancements will matter if we cannot protect our communication from our enemies. “One thing we can be sure of in our next fight is that our adversaries will be more sophisticated in cyber warfare,” declares BG Hughes. As cyber-attacks become more and more frequent among unstable regions across the globe, communication security becomes more and more important for national defense. Current tactical communication devices require strong passwords, but even the most complex password is only a single-factor form of authentication. NaN systems employ a simplified authentication mechanism, eliminating the need for multiple passwords to sign on to the network and increasing cybersecurity using biometric identification methods. Future warfighters can expect to provide advanced multi-factor authentication, including facial recognition and iris scans coupled with one-time passwords or tokens. Additionally, NaN systems communicate via protected satellites using anti-jamming technology. Key encryption is currently the primary means of securing satellite transmissions. Future satellites resemble Advanced Extremely High Frequency Milstar satellites that employ a spread-spectrum approach called adaptive nulling, in which the signal hops in pseudo-random fashion from frequency to frequency within an assigned bandwidth.

Leaders across the operational force will

(Continued on page 6)

(Continued from page 5)

experience a steep learning curve, as they say goodbye to the equipment they were initially trained on and used during a decade of combat operations, and are introduced to equipment with a whole new look and feel. OIF and OEF produced tactically tested war fighters who are now leaders of our maneuver forces, and these leaders have become accustomed and comfortable with the use of combat net radios (SINGARS, TACSAT, FBCB2) to enable mission command. The fielding and training efforts entrenched in the network modernization roadmap must result in a high level of comfort among brigade and battalion leadership in order to prevent leaders from dusting off their old MBITRs and ASIPs and reverting to operating how they are comfortable.

The network is fundamental to a smaller, highly capable



CPT Jonathan Page, a troop commander with the 4th Brigade Combat Team, 10th Mountain Division (Light Infantry), uses a rifleman radio and Nett Warrior end user device, at Nangalam Base, Afghanistan, in 2013. After fielding initial rifleman radios as part of the Capability Set 13 and 14 communications suite, the Army is moving forward to procure additional radios through full and open competition

Army that faces the increasingly complex enemy of tomorrow. The Network Modernization Roadmap illustrates the Army's strategy to fill capability gaps and make necessary improvements to network functionality that ensures American Soldiers

remain the most lethal fighting force on the battlefield. It is clear that the army has committed great time and resources toward modernizing our tactical communication architecture, but teaming up with the tacticians who are developing the force structure of 2025 is the most valuable initiative. The network of 2025 is no doubt more advanced, yet simpler to operate than our current network. Despite technological advancements, the tactical network's purpose remains constant – a means through which commanders exercise immediate and personal control over their forces.

CPT Kyle D. Barrett is an Army Signal captain serving as a senior Signal observer controller trainer at the Joint Multinational Training Center. CPT Kyle has served as a company fire support officer, mortar platoon leader, battalion fire support officer, and Signal company commander.

ACRONYM QuickScan

AEHF – Advanced Extremely High Frequency
ASIP – Advanced System Improvement Program
CERDEC – Communications – Electronics Research, Development and Engineering Center
CP – Command Post
CS 14 – Capability Set 14
FBCB2 – Force XXI Battle Command Brigade and Below
JBC-P – Joint Battle Command – Platform
JCR – Joint Capability Release
LTE – Long Term Evolution
MBITR – Multi Band Inter Intra Team Radio
MDL – Mission Data Loader
NAN – Network after Next
NetOps – Network Operations
OEF – Operation Enduring Freedom

OIF – Operation Iraqi Freedom
PEO C3T – Program Executive Officer for Command, Control, and Communications – Tactical
PoP – Point of Presence
SINGARS – Single Channel Ground and Airborne Radio System
SNE – Soldier Network Extension
STARNet – Simplified Tactical Army Reliable Network
SRW – Soldier Radio Waveform
TACSAT – Tactical Satellite
VLAN – Virtual Local Area Network
VPN – Virtual Private Network
STARNet – Simplified Tactical Army Reliable Network
WIN-T – Warfighter Information Network – Tactical

SIGNALEERS AT WORK



If there is anyone who thinks that Signal Soldiers are stuck in dark closets with banks of computers and telephones far from the action of military maneuvers this will offer an eye opener. From around the world in this issue are photographs of Signal practitioners working in the field.

(Above) U.S. Signal Soldiers provide security and communications during an advising visit to the police regional logistics center in Afghanistan's Nangarhar province.

(Right) CPL George Huley, discusses proper trigger-pulling techniques with PVT Noel Toye during the rifle qualification portion of the 3rd annual U.S. Army SPC Hilda I. Clayton Best Combat Camera event on Fort Meade, Md. The two are combat documentation/production specialists assigned to the 55th Signal Company.



Implementing Policies...

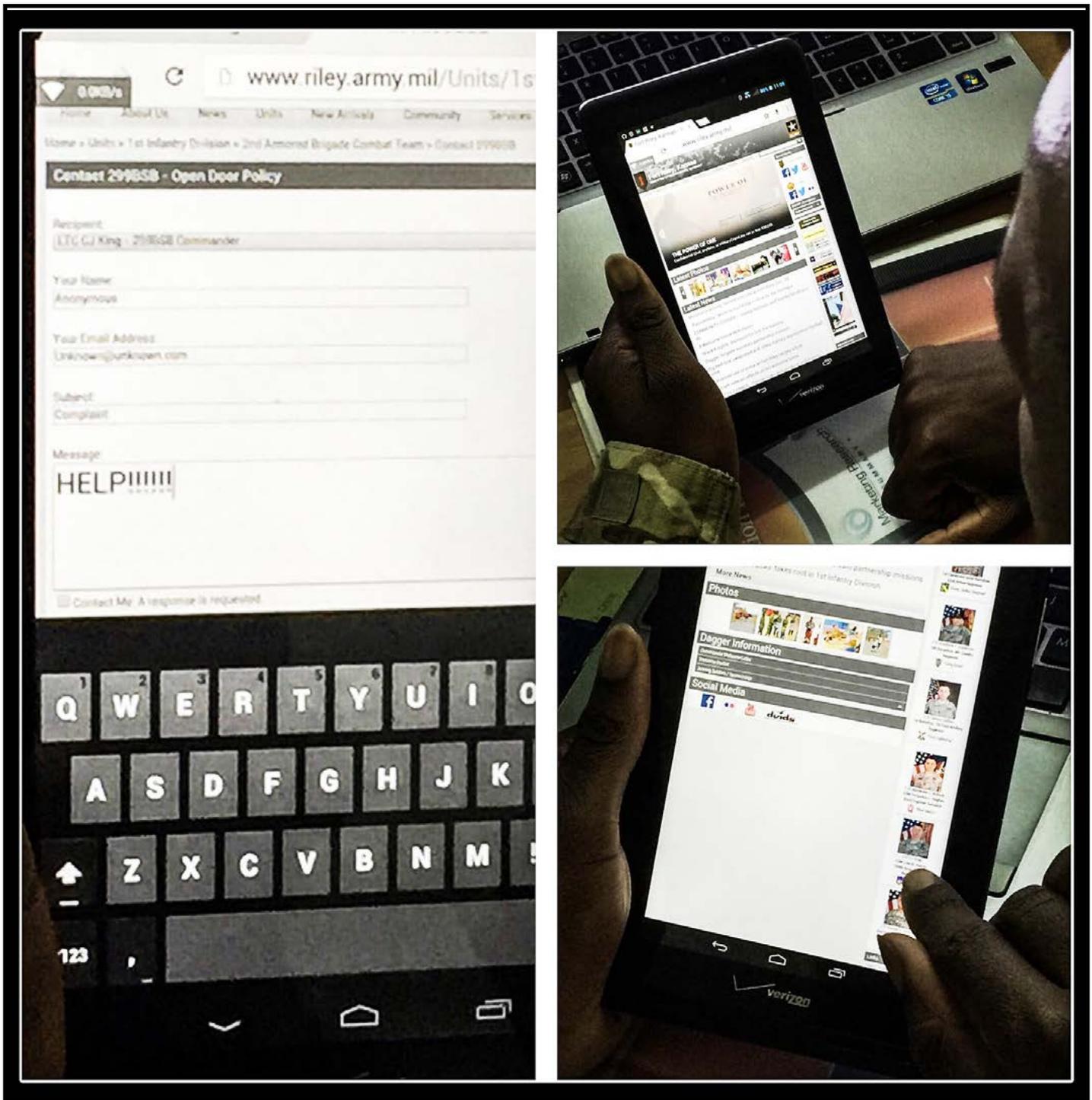


By CPT Trenin D. Spencer,
SFC Christopher L. Donald
SPC Ashley M. Ardiana

Computers have the ability to maximize work efficiency while reducing the costs of operations, which makes emerging military computer applications and ideas to leverage existing technologies for multiple military uses extremely desirable for our military.

From battle tracking, fires integration, and airspace de-confliction to personnel management, education, and training management, the U.S. military has already integrated computers into the majority of its daily operations and will move to do so on an even greater scale as the ever evolving threat to our country mushrooms across all technology-enabled pathways.

...Electronically



(Above top right) A Soldier uses a personal electronic device to access the Open Door Policy via the Fort Riley, Kansas official webpage. (Above left) The picture displayed on the personal electronic device is of a filled in contact form. (Bottom right) The picture displayed on the personal electronic device is of the battalion commander's page located on the Fort Riley, Kansas official site.

(Continued from page 8)

As our military continues to modernize through the integration of computer technologies into daily operations, the implementation of military policies using electronic means is the future of the Army, and the exercise of the universal policy letter #1: Commander's Open Door Policy, utilizing the existing army enterprise email infrastructure, is the first leap toward that future.

Recently LTC C.J. King, battalion commander 299TH Brigade Support Battalion, 2ND Armored Bridge Combat Team, 1ST Infantry Division, made the comment that he felt "his open door policy was not effective, because it was not being utilized" and wished there was a better way to implement the policy.

Across the military, there is a shared misconception that as long as the door to the commander's office is open and the commander is not otherwise engaged, then the commander's open door policy is being exercised, and if Soldiers have legitimate issues, they will recognize the open door and address the issues.

As it turns out, that is definitely not the case as there are several barriers that deter Soldiers from exercising the open door policy. Those barriers most notably include intimidation of raising concerns to O-3 and above Officers and E-8 and above Noncommissioned Officers, and also fear of reprisal from the Soldier's immediate supervisor. As a result of LTC King's comment, SFC Christopher L. Donald (communications chief for the 299TH Brigade Support Battalion, 2ND Armored Bridge Combat Team, 1ST Infantry Division) devised a method for Soldiers to use the battalion commander's open door policy anonymously by accessing the publicly available official Fort Riley, Kansas, 1ST Infantry Division, "BIG RED ONE" website, and clicking on a hyperlink located on the battalion commander's command profile, which sends an unaddressed email to his army enterprise email address. This method of exercising the open door policy is not only completely confidential between the Soldier reporting and the battalion commander, but unless the Soldier chooses to include contact information in the message of the email, there is also no way for anyone else to know who exercised the policy. Due to the immediate success of the electronic form of open door policy, the battalion

command sergeant major, company and battalion commanders across the division, and a commander in the Air Force all requested similar programs within weeks of our implementation.

Following implementation, it was quickly found that the ability to send anonymous emails to the battalion commander not only eliminates the intimidation and fear of reprisal barriers that Soldiers face, but it also provides the battalion commander with insight that he might not gain through vocal conversation due to a Soldier's inability to express him or herself orally. Other benefits discovered as a result of the electronic implementation of the open door policy include the increase in availability of the commander to address issues and the ease of use to exercise the policy for all Soldiers.

Commanders are busy Soldiers! Prior to the electronic implementation of the open door policy, the battalion commander was only available to discuss issues for potentially an hour during the duty day, and maybe an hour or two afterwards. The electronic open door policy completely removed time restrictions to address issues. All commanders have government issued personal electronic devices, such as Blackberry or iPhone devices, literally attached to their hips almost twenty-four hours a day. The electronic devices, coupled with the electronic open door policy, gives commanders immediate and twenty-four hours access to Soldiers who choose to utilize the open door policy.

Prior to the electronic implementation of the policy, geographical location limited the use of the open door policy. Soldiers who operate away from the flagpole, and who do not have the opportunity to interact with the command on a daily basis do not possess the ability to exercise the traditional open door policy and bring up the issues that often arise in isolated environments.

The electronic open door policy diminishes the effect of geographical separation and increases the ease of use of the policy for all Soldiers, because it only requires internet connectivity, a commonality for Soldiers to possess twenty-four hours a day in this age of the computer.

The electronic open door policy is easily integrated into standing policies. To set up your electronic open door policy you simply need to follow these steps:

1. Coordinate the creation of an email distribution list containing your policy owner/ owners information (battalion commander, command sergeant major, etc.) with your installation's Network Enterprise Center by submitting a work order. Your NEC will coordinate with the Army Enterprise Service Desk and reply with the work order that is created in order to begin the process. It takes about 3-5 business days for the distribution list to be created.

As a best practice, your local automations personnel (S6) should manage the distribution list once it has been created.

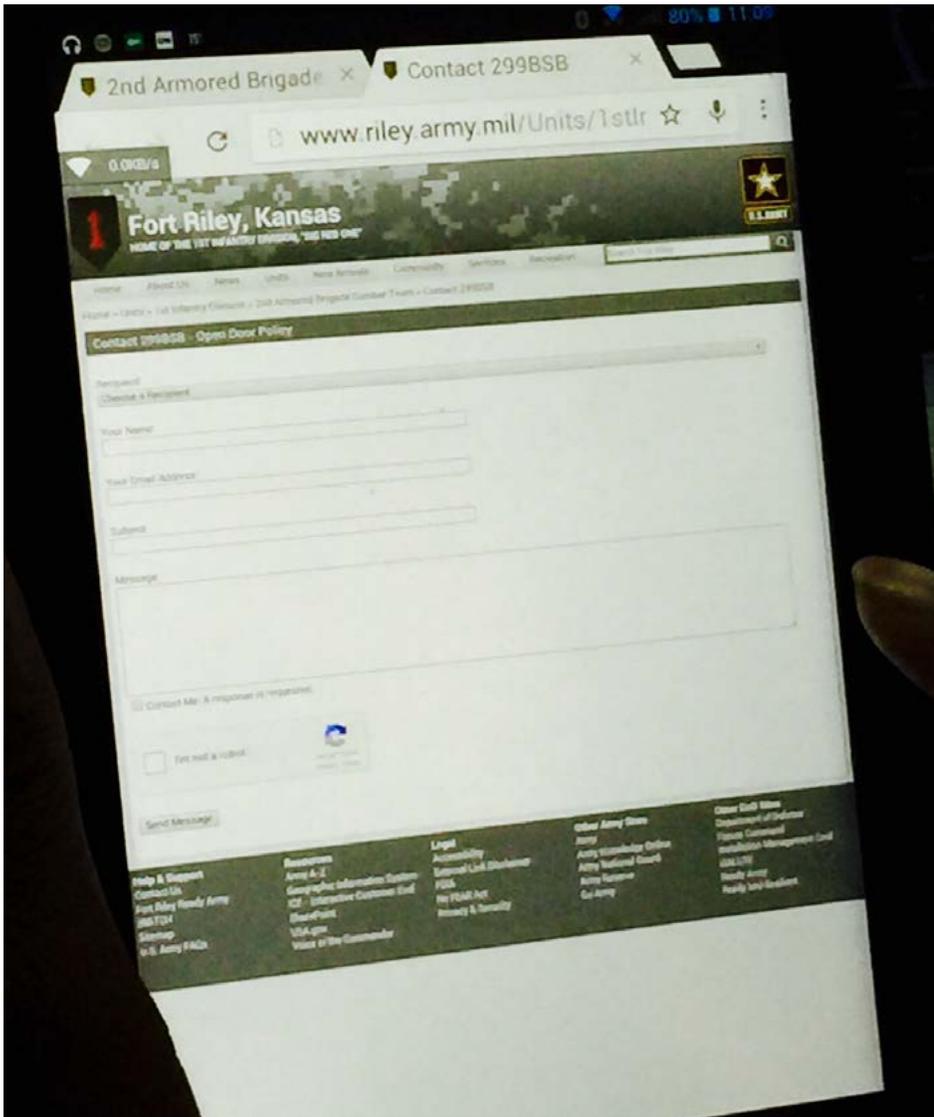
2. Once you receive the email stating that the distribution list has been created, you need to contact your installation public affairs office web administrator. The PAO web administrator is in charge of managing your installation's official web page. From your PAO web administrator, you will request

the creation of a hyperlink that accesses a web based contact card or form using the policy owner's name. The contact card/ form will contain the following information:

- i. RECIPIENT: choose the policy owner, or if multiple leaders are using the same link, you may choose your leader of choice via dropdown menu;
- ii. YOUR NAME: you may put anonymous or your own name if you would like to make the recipient aware of whom he or she may contact;
- iii. YOUR EMAIL ADDRESS: you may either use your government email address, a personal email address, or a completely fake email address;
- iv. SUBJECT: The concern you would like to make known to the recipient;
- v. MESSAGE: Explanation of the concern and what suggestions you have regarding the concern.

3. The hyperlink is to be located on the policy owner's unit's official page. As a best practice, locating the hyperlink beneath the official command photograph allows for quick and simple access, without the hassle of searching every inch of the webpage. The link takes approximately 3-5 business days to be fully operational.

4. Finally, after you have received an email stating the link is good to go, you will then need to test the link. As a best practice, initially you must hold the control button and refresh the web page at the same time to get the link to work properly. Once the link for the contact card/ form is up and running, you will then be able to post how-to instructions throughout the unit to show Soldiers how



This display shows how a Soldier can use a personal electronic device to access the Open Door Policy via the Fort Riley, Kansas official webpage. The picture displayed on the personal electronic device is of a blank contact form.

(Continued on page 12)

(Continued from page 11)

to utilize the new open door method.

Best practices to ensure widest dissemination of the electronic open door policy include flyers posted in all work and barracks areas detailing instructions on how to access the anonymous email hyperlink, briefings on the policy at weekly closeout formations, and even the Family Readiness Group channels.

In addition to reminding Soldiers about the policy during the weekly closeout formation, using that time to acknowledge receipt of issues brought up as a result of the open door policy, and to request additional information in order to action issues of major concern are also proven best practices.

Overall, the electronic open door policy is easy to manage and enjoys seamless integration with current policies, however it does require some overhead maintenance. It is important to ensure that email configurations are reconfigured with changes in command or key personnel, or else you end up standing tall in front of a very upset command sergeant major attempting to explain why the prior command

is being notified about issues within the current command.

There is no mistaking that this is the age of the computer. Computer technology, which is nowhere near the pinnacle of its potential, will continue to shape the battlefield for decades to come. Soldiers of the 1ST Infantry Division, Big Red One or BRO Soldiers, understand and embrace this at every level. 1ST Infantry Division Commanding General, MG Wayne W. Grigsby, uses a commander's digital dashboard to post information and enable dialogue while flattening the organization, BRO leadership use computer technology such as the Digital Training Management System and the Army e-Learning Program to manage and supplement training, and BRO Soldiers use computer technology such as the Engagement Skills Trainer and convoy simulators to maintain lethality and readiness, making the 1ST Infantry Division the most Brave, Responsible, and On Point division in the Army. The exercise of Army policies via electronic means is here, and the electronic open door policy is the first of many policies to come as our Army continues to advance in this age of the computer.



**2nd Armored Brigade Combat Team
"Dagger Brigade"**

CPT Trenin Spencer is the communications officer for the 299th Brigade Support Battalion, 2nd Armored Brigade Combat Team, 1st Infantry Division., Fort Riley, Kansas. He previously served as the signal company commander for the 2nd Armored Brigade Combat Team, and the communication's officer for 1-7 FA, 2ABCT, 1ID. His deployments include Kuwait, Malawi, Mauritania, and Iraq.

SFC Christopher Donald is the communications section chief for the 299th Brigade Support Battalion, 2nd Armored Brigade Combat Team, 1st Infantry Division, Fort Riley, Kansas. He previously served as the platoon sergeant for G6, 21st Theater Sustainment Command, Kaiserslautern, Germany. His deployments include 2x Kuwait, 3x Iraq, Bosnia, and Kosovo.

SPC Ashley Ardiana is the senior local area network manager for the 299th Brigade Support Battalion, 2nd Armored Brigade Combat Team, 1st Infantry Division., Fort Riley, Kansas. She previously served as LAN manager for Headquarters and Headquarters Battalion, 2nd Infantry Division, Camp Red Cloud, South Korea.

ACRONYM QuickScan

ABCT – Armored Brigade Combat Team
BRO – Big Red One
FA – Field Artillery
LAN – Local Area Network
LTC – Lieutenant Colonel
NEC – Network Enterprise Center
NCOIC – Non-Commissioned Officer In Charge
PAO – Public Affairs Officer

SIGNALEERS AT WORK



(Above) U.S. Army LTC Jim Urbec shouts commands to paratroopers as they prepare to jump from a CH-47 Chinook helicopter during a static line airborne operation over Homestead Air Reserve Base, Fla. LTC Urbec was the director of communications assigned to Special Operations Command South.



(Left) U.S. Army SPC Colby Welch sets up radio communications inside an abandoned fortress in Petawa village in Afghanistan's Parwan province. Welch is assigned to the 101st Airborne Division's Company A, 1st Battalion, 2nd Brigade Combat Team, Task Force Strike.

Lessons Learned



*By LTC P.K. Sayles
MAJ Daniel J. Kull*

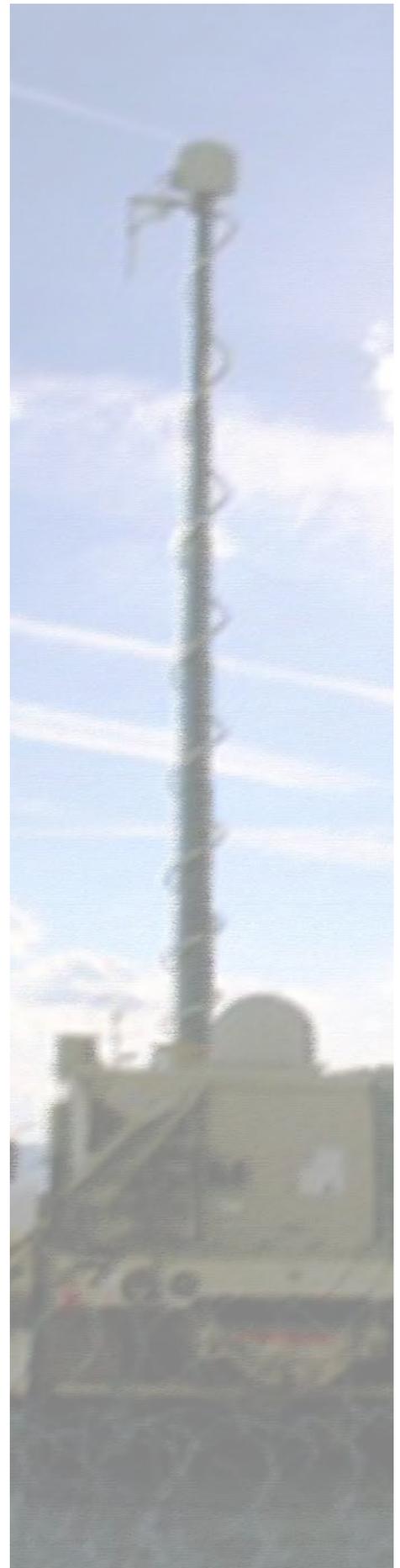
This article reveals the challenges and shares lessons learned in overcoming the hurdles of deploying with one communications capability and transitioning to a newer package.

In October 2014, the headquarters of First Infantry Division deployed to Iraq in support of Operation Inherent Resolve with its full complement of Warfighter Information Network – Tactical communications equipment.

WIN-T is an ever-evolving U.S. Army program that provides mission command networking at tactical and operational echelons.

We deployed with WIN-T Increment 1b, which includes joint network nodes supporting users at the division's mission command posts and a single tactical hub node connecting the JNNs to the Department of Defense Information Network.

But the Army is in the midst of a transition to WIN-T Increment 2, which comes with new equipment and new doctrine for the employment of that equipment. In the middle of the forward deployment, 1ID was operating astride Increment 1b, with which it deployed, and Increment 2, which many of its subordinate units possessed.



(Continued from page 15)

The Army began fielding WIN-T Increment 1a in 2004 to update its aging Mobile Subscriber Equipment.

With Increment 1a, command post nodes provided connectivity to battalions, JNNs provided connectivity to brigades and divisions, and a series of satellite and line-of-sight circuits connected them to each other and to the divisional THN.

The Army also established five Regional Hub Nodes around the world to provide connectivity to the DODIN during the initial stages of an operation before divisions could install their THNs. With this baseline firmly in place, the Army began fielding Increment 1b in 2013 to add some additional capabilities and to help bridge the gap to Increment 2.

The Army has been fielding Increment 2 since 2013 and will continue fielding it to units as their deployment schedules allow for the next few years.

Increment 2 includes new equipment for all echelons: Tactical Communications Nodes replace JNNs and CPNs at the division, brigade, and battalion echelons, points of presence and Soldier network extensions extend connectivity to the company echelon and RHNs require hardware upgrades to interface with these new systems. There is no direct replacement for the THN with Increment 2, as the TCN in conjunction with the RHN obviates the need for a division THN.

Because of that, the Army can divorce THNs from a divisional support role, retain them in a strategic reserve, and deploy them as mobile RHNs to areas that either lack RHN coverage or require a layer of redundancy.

Therein is the friction. From a doctrinal perspective, the impending obsolescence of the THN puts more importance on the RHNs, as divisions now must remain reliant on the RHN throughout the duration of an operation. From a practical perspective, the present paradigm in which the Army stands astride Increment 1b and Increment 2 necessitates that the RHN be able to support both sets of systems. But how can RHNs take the time to upgrade their hardware to support Increment 2, when it must remain engaged to support divisions operating on Increment 1b?

The Challenge of Changing Doctrine

Before deploying, we planned the division network according to Increment 1b doctrine; that is, we projected our THN to remain in Kuwait and configured our JNNs to link to them. In accordance



CW2 Demetrius Council, from 3rd BDE 82nd Airborne Division, demonstrating WIN-T Increment 2 for LTC P.K. Sayles, the CJFLCC-I CJ6.

with this plan, we initially aligned our JNNs to connect to the DODIN, and to each other, via the RHN at Camp Arifjan. In December 2014, as we prepared to swing our satellite links to our THN, we learned that network enterprise technology command, in anticipation of the transition to Increment 2, was pioneering a doctrinal change that precluded the use of our THN.

This doctrinal change was tenable for many reasons. By remaining on the RHN, we enjoyed the support of a large and experienced staff of civilian technicians at the RHN with better assurance of network security and we would be ahead of the doctrinal changes that Increment 2 would bring. In effect, our deployment would validate the paradigm shift.

The doctrinal change also presented a challenge for us. With the THN we had total control of that end of the network and could implement a number of measures to improve the quality of the network. We could configure a logical mesh of our satellite circuits to reduce latency. We could also optimize circuits to mirror tactical priorities and exercise end-to-end control of our network. With the THN we had a layer of redundancy to enhance network survivability and we would not have to compete for support with the myriad additional customers that the tireless staff at the Camp Arifjan RHN services. How could we achieve all of the advantages that the THN would

have provided us without using our equipment?

First, we worked closely with the Camp Arifjan RHN to configure a logical mesh for our satellite circuits. This reduced latency among our bases by half. Before the implementation of this mesh, the signal flow required two satellite “hops” (from the JNN in Iraq to the RHN at Camp Arifjan, and back). After the implementation of the satellite mesh, the signal flow required only one “hop” (the transmitting JNN in Iraq could link directly to the receiving JNN in Iraq).

As our technicians configured the mesh we coordinated with the leadership of the Camp Arifjan RHN to ensure that we had sufficient control over the network to support the commander’s tactical priorities. At NETCOM’s direction, we obtained veto authority on Authorized Service Interruptions, which the RHN conducted periodically to perform maintenance on their hardware. We also formulated a Service Level Agreement with the RHN that allowed 1ID technicians to work inside the RHN to support 1ID’s network and we tweaked the reporting procedures to establish reporting channels that included 1ID.

These were all makeshift solutions to emerging problems. These solutions were successful in that 1ID was able to communicate throughout the breadth of Iraq during this deployment. But the concepts that led to these solutions were underdeveloped and inefficient, consuming more time and resources than we would have used had we simply employed our THN. It is evident that there is a need for further development of doctrine as battlefield commanders outsource their communication capabilities

to theater Signal commands far in the rear.

The Challenge of Disparate Equipment

The integration of Increment 2 into an Increment 1b network and the hardware requirements that Increment 2 places on the RHN presented a challenge. When OIR began, the Camp Arifjan RHN had not yet updated its hardware to accommodate the increased capabilities of Increment 2. So as subordinate units deployed into theater with Increment 2 systems, they connected to the RHN’s legacy hardware and lost the additional advantages of Increment 2; such as Mission Command on the Move technology.

The hardware upgrade that the RHN required would entail multiple ASIs, of up to three hours each, during which the RHN would not be able to support 1ID. As we noted above, NETCOM had entrusted 1ID with veto authority over ASIs and we valued the ongoing mission against Da’ish more than the Increment 2 capabilities that the upgrade would provide. So we used this veto repeatedly as the RHN tried to schedule these ASIs. It quickly became clear that there were very few windows of opportunity to execute these ASIs. A three-hour ASI is a tall order and with 1ID engaged in a continuous fight we were unwilling to risk isolating warfighters to accomplish this upgrade.

This intractable dilemma revealed another shortfall of the current doctrine for Increment 2 – the RHN is a single point of failure. There are no alternate sites to land our satellite shots and so each ASI was tantamount to a network blackout at the

tactical edge of the battlefield.

Ultimately, we endured the hardware upgrade to the RHN through three separate ASIs. The ASIs were of successively greater impact to us. The first ASI had a minor impact on us as it affected only a couple of our terminals, while the last ASI affected 27 of our terminals and had a profound impact on us. Fortunately, we learned from our mistakes and accrued institutional knowledge as we progressed through the ASIs, so that the RHN was able to execute the third ASI with efficiency and aplomb. The proof is in the outage times. The first ASI lasted over five hours, the second ASI lasted four hours twenty minutes, and the third ASI last three hours twenty-nine minutes.

What did we do wrong in the first ASI that we were able to correct by the third ASI? We improved our preparation for the ASI by conducting rehearsals and refining the step-by-step script for the ASI. We also improved our coordination with terminal operators to ensure we had timely responsiveness as we tested services at each site.

The most important change we made was our decision to accept risk to the network to mitigate risk to the mission. Part of the RHN upgrade was a new firewall; in the first two ASIs, we spent most of our time adding firewall modifications, line by line, for every service at every terminal. This extended the outage and incurred risk to the mission (and risk to the force; how quickly could we respond to troops in contact with the enemy if we could not communicate?). For the third ASI, we refused to accept this risk to the mission and insisted that the

(Continued on page 18)

(Continued from page 17)

RHN accept risk to the network instead. The firewall remained open by default, and technicians at the RHN feverishly worked to add firewall modifications for our terminals so that they could close the firewall to protect the network. Until the technicians closed the firewall, the network remained exposed to risk; but the benefit of this risk was the mission command capability that we maintained during the ASI. The risk to mission outweighed the risk to network.

Recommendations

We have identified three significant issues wherein doctrine has not kept pace with technology and below are recommendations to address those issues.

First, commanders must be able to assert control of their mission command ability and this implies some level of cooperation with the theater signal command. The theater signal command must genuinely support the maneuver commanders and respond swiftly to battlefield priorities. The principle of unity of command dictates that commanders should be able to control their own destiny with something as important as communications. Furthermore, it should not be in the purview of a theater Signal command to

suspend the communications between a supported commander and the supported commander's subordinates on the battlefield without that commander's concurrence and so this requires conferring upon the maneuver commander a veto authority for all ASIs.

Second, the RHN must have internal, automatic failover capability. This includes not only automated failover among the divisional enclaves within the RHN, but also from the RHN to another hub node. This redundant hub node may be another Regional Hub Node, or an Area Hub Node, or (until the Army re-purposes divisional THNs) the deployed division can furnish its THN to the RHN for implementation as a redundant system.

Third, the Army must be able to balance the competing priorities of short-term mission requirements and the long-term investment of upgrading equipment. Technology will continue to progress and so there will always be a need for equipment upgrades. The Army must have the institutional agility to conduct equipment upgrades while still seamlessly executing its missions. It would be strategically foolhardy to accept degradation to operations – the *raison d'être* of technology upgrades – in order to accomplish the upgrade.

Above all, the Army must

inculcate this attitude into its leadership. It is myopic to eschew technology upgrades for the sake of an operation; it is no better to eschew the operation in favor of the upgrade. There is a balance between the two, and it takes astute leadership to strike that balance.

LTC P.K. Sayles served as G6 of First Infantry Division from April 2013 to July 2015; she was dual-hatted as the CJ6 of Combined Joint Forces Land Component Command – Iraq from October 2014 to July 2015. She has served as a Signal officer in multiple strategic and expeditionary commands, including Current Operations Chief at International Security Assistance Forces Joint Command and the director of Joint Network Control Center – Afghanistan. She is currently the Signal Branch Enlisted Chief at U.S. Army Human Resources Command.

MAJ Daniel J. Kull served as Network Operations Officer for Combined Joint Forces Land Component Command – Iraq from October 2014 to June 2015. He has accrued extensive tactical Signal experience during his 26 months in Iraq; he has also accrued 24 months of strategic Signal experience in Korea. He is currently the S-6 of 1st Brigade, 1st Infantry Division.

ACRONYM QuickScan

1ID – First Infantry Division
ASI – Authorized Service Interruption
CPN – Command Post Node
DODIN – Department of Defense Information Network
JNN – Joint Network Node
NETCOM – Network Enterprise Technology Command

OIR – Operation INHERENT RESOLVE
POP – Point of Presence
RHN – Regional Hub Node
SNE – Soldier Network Extension
TCN – Tactical Communication Node
THN – Tactical Hub Node
WIN-T – Warfighter Information Network – Tactical

Global Response Force Exercises

Flying Command Post



(Photo by Amy Walker)

Soldiers set up the Army's Enroute Mission Command Capability network equipment onboard a C17 aircraft in preparation for a capability demonstration. The Soldiers are, from left to right, CPT Kristen Jones (product lead for EMC2), CPL Derick Peterson, 1LT Mike Laquet and SGT Jonathon Bennett.

By Amy Walker

During a recent large-scale Joint Forcible Entry exercise, paratroopers from the 1st Brigade Combat Team, 82nd Airborne Division and the Assault Command Post unit of the XVIII Airborne Corps leveraged the Army's networked Enroute Mission Command Capability to obtain the inflight mission command and plane-to-plane, plane-to-ground communications needed for a successful parachute assault.

"EMC2 provided the airborne assault force with the ability to maintain situational awareness and to collaborate with their higher headquarters and joint partners all the way to the objective," said COL Timothy Watson, assistant chief of staff for XVIII Airborne Corps G3 (operations).

By leveraging technologies similar to those used by today's commercial airlines to provide inflight internet access, EMC2 enables the Global Response Force of the XVIII Airborne Corps and 82nd Airborne Division to access the mission command and secure network communications enabled by the Army's tactical communications network, Warfighter Information Network-Tactical. While in flight paratroopers can also view situational awareness,

such as Unmanned Ariel Vehicle feeds of the drop zone, in real-time on large LED screens mounted inside the plane so they are better prepared to fight on arrival.

"EMC2 enables mission command for the GRF and joint partners over strategic distances," Watson said. "It facilitates secure voice and data services, collaborative planning, up-to-date situational awareness and informed decision making for the GRF and joint partners while en route to the objective area."

The large-scale joint Army/Air Force JFE operation was part of a capstone exercise for the Air Force Weapons School and employed approximately 400 paratroopers and 100 aircraft. It was designed to mimic a joint forced entry scenario. During the exercise, GRF Soldiers successfully employed EMC2 while en route from Fort Bragg, N.C. to Nellis Air Force Base, Nevada.

The GRF has successfully utilized EMC2 to support several other JFE exercises across the United States including the National Training Center at Fort Irwin, Calif. in July 2015, and during Bold Quest, which took place in October 2015 at Fort Bliss, Texas. "The Army and joint services are working to provide network connectivity at every stage of operations,



During a Joint Forcible Entry exercise, Global Response Force Soldiers successfully employed Enroute Mission Command Capability while en route from Fort Bragg, N.C. to Nellis Air Force Base, Nevada.



(Photo by CPT Lisa Beum)

Paratroopers are well prepared to jump during the large-scale joint Army/Air Force Joint Forcible Entry exercise in December 2015, where Soldiers successfully employed Enroute Mission Command capability, while en route from Fort Bragg, N.C. to Nellis Air Force Base, Nevada. This network communications capability enabled the unit to obtain the inflight mission command and plane-to-plane, plane-to-ground communications needed for a successful parachute assault.

and EMC2 provides that missing communications link while deployed in the air, whether that is en route to a hostile military engagement or for humanitarian aid during disaster response,” said LTC Mark Henderson, product manager for WIN-T Increment 1, which manages EMC2 for the Army.

During all of these JFE exercises, EMC2’s broadband reach-back capability enabled classified web-based enterprise services such as such Defense Collaboration Services (Web conferencing and chat), email, secure voice over internet protocol and SharePoint. Since all of these tools are joint, it makes continued after station collaboration between Airborne leaders and the Air Force possible. Additionally, when needed, EMC2 can securely and easily connect to the coalition network.

“Real-time situational awareness is challenging to obtain during long transit times to an objective,” said MAJ Jason

Murray, 18th Field Artillery brigade, 82nd ABN Div. “Having the ability to communicate

(Continued on page 22)



(Photo by CPT Lisa Beum)

LTC Mark Henderson, product manager for Warfighter Information Network-Tactical Increment 1, works with his Enroute Mission Command Capability Team onboard a C17 aircraft in flight during a Joint Forcible Entry exercise in December 2015.

(Continued from page 21)

during flight gives the paratroopers and commanders an enhanced understanding of what they are about to encounter, allowing them to be more effective once they reach their destination.”

Murray’s unit plans, synchronizes, and employs long range precision strike fires and counterfires in support of the XVIII Airborne Corps and Special Operations forces as required. During the recent JFE exercise, the Army utilized EMC2 in support of fires missions for the first time.

“As a joint fire support officer I am very concerned about the pre-assault fires that happen before we get to the drop zone,” Murray said. “Having EMC2 enables us to track the execution of pre-assault fires and their effects on the enemy before we arrive.”

The GRF utilized a mission command fires planning tool called Joint Automated Deep Operations Coordination System, which was integrated for the first time on EMC2’s Key-leader Enroute Node. JADOCs is a joint and coalition Windows-based software suite that provides integration and synergy between multiple joint and coalition forces for real-time targeting and fires coordination.

“Having JADOCs airborne enabled the XVIII Airborne Corps to synchronize artillery and missile fire, evaluate their effects, and refine the mission plan with multiple echelons of leadership in different locations and services, all as they approached the objective,” said 1LT Mike Laquet, 50th Signal Battalion (Expeditionary) platoon leader, who oversees the operation and maintenance of the EMC2 equipment. The XVIII Airborne Corps plans to continue to use JADOCs as a part of their EMC2 mission command application suite.

Since the GRF must rapidly deploy anywhere in the world with little to no notice, they need as much situational awareness as possible. Prior to EMC2, these forces had previously been without robust



(Photo by CPT Lisa Beum)

A Global Response Force paratrooper utilizes the Army’s Enroute Mission Command Capability for inflight situational awareness from Fort Bragg, N.C. to Nellis Air Force Base, Nevada, before jumping during parachute assault at the Army/Air Force Joint Forcible Entry exercise.

communications or had little bandwidth to support mission command applications during flights that could last up to 18 hours.

“The real time connectivity we provide to classified network services gives a level of situational awareness that was previously unheard of en route to the drop zone,” Laquet said. “EMC2 gives the leadership of XVIII Airborne Corps the ability to have mission critical information up to the point where they exit the door.”

Amy Walker is a staff writer for Data Systems Analysts Inc. supporting the Army’s Program Executive Office for Command, Control and Communications-Tactical; project manager Warfighter Information Network-Tactical and MilTech Solutions. She graduated from The College of New Jersey, Ewing, N.J. She has covered the Army’s tactical network for nearly 10 years, including multiple test and training events.

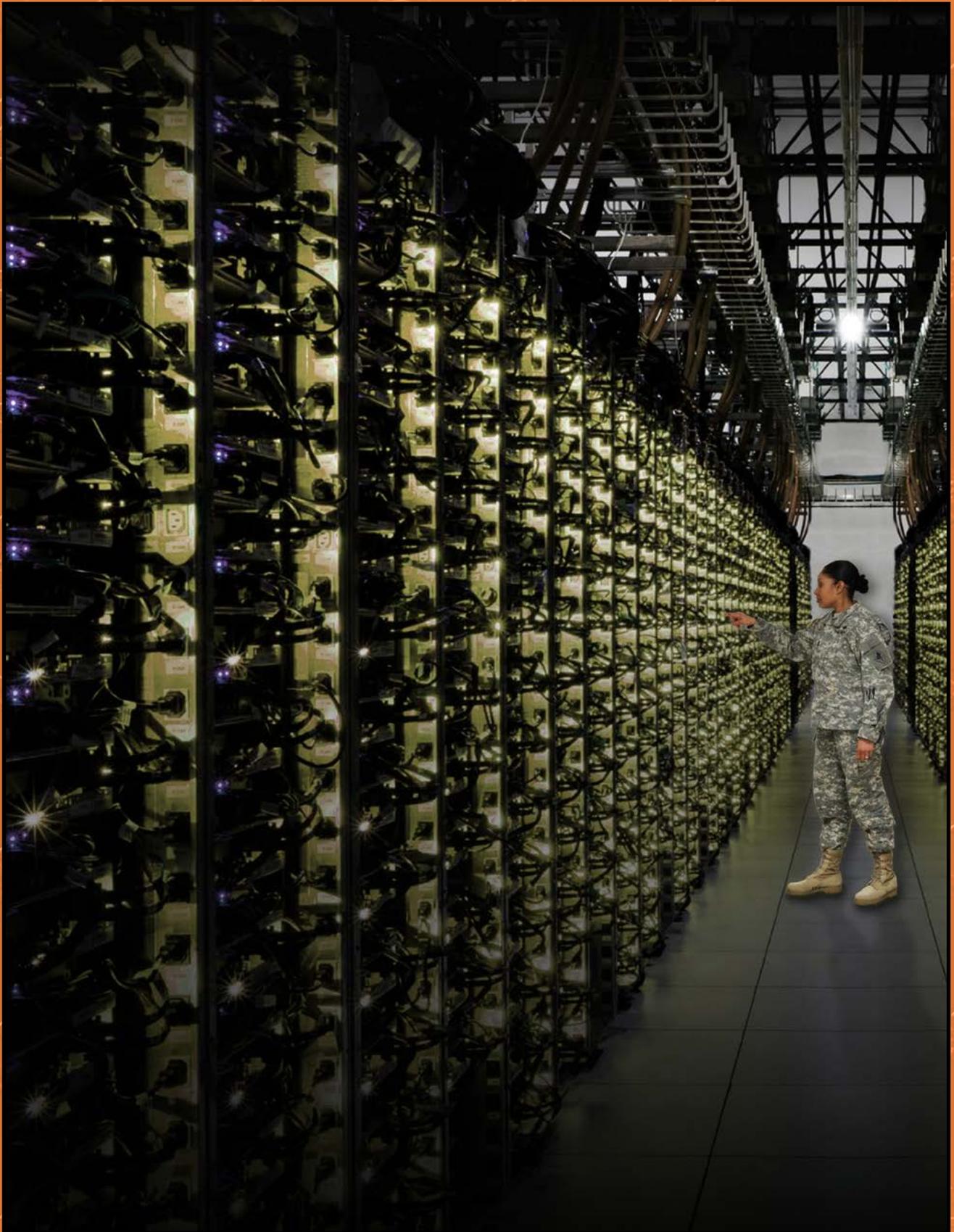
ACRONYM QuickScan

ABN Div - Airborne Division
EMC2 - Enroute Mission Command Capability
GRF - Global Response Force
JADOCs - Joint Automated Deep

Operations Coordination System
JFE - Joint Forcible Entry
KEN - Key-leader Enroute Node
PEO C3T - Program Executive Office for Command, Control,

Communications-Tactical
SVOIP - secure voice over internet protocol
WIN-T - Warfighter Information Network-Tactical

SIGNALEERS AT WORK



MSG Tanisha Aiken, senior career management noncommissioned officer for visual information, works in a simulated bank of network servers.

Meeting Real-World Challenges

Signal Support to Infantry Combat Teams



By CPT Vernon Pittman

The Infantry brigade combat team Signal company has the mission “To provide 24-hour operational Command, Control, Communications, Computer, Intelligence, Surveillance, and Reconnaissance signal systems network to the supported Infantry brigade combat teams..., which includes deploying, installing, operating, and maintaining these systems.”

With the current, authorized, organization and equipment it is extremely challenging, if not impossible, for the company to accomplish this mission.

For example, the unit lacks the Soldiers and expertise needed to run effective 24-hour operations with the Tactical Communications Node. Further, the unit is forced to “come out of hide” to fill a Soldier Network Extension crew, which compounds the stated 24-hour operation issue. Also, the Signal company has also lost all staff sergeants.

Finally, the unit has retained legacy

communications systems and vehicles without the Soldiers to operate or maintain them.

Interestingly, the problem is not one that needs a remarkable increase in the number of personnel to solve. There are two varied and distinct ways that we can solve this dilemma. The first is by altering our structure slightly and adding some key positions, and the second is eliminating the structure altogether.

The Problem...Strength

Since Fiscal Year 2005 the IBCT Signal company has been the victim of a progressive and approximately 40% reduction in strength (see Figure 1).

Presently, the unit stands at an authorized strength of 35 with three officers, nine non-commissioned officers, and 23 E-4 and below. Some of the reduction is due to Army-wide changes such as removing organic Chemical, Biological, Radiological, Nuclear and Electrical NCOs from unit headquarters however, that is not the full story.

Additional Duties

Further, the low strength of the Signal Company overcomplicates additional duty management and mandatory training requirements. Generally there are approximately 43 additional duties that a company must fill (see Figure 2).

Most of the duties have primary and alternate positions associated with them. Of these duties, the company can fill roughly five with E-4 and below, and three with an O-2. This means that the vast majority of additional duties (roughly 35) fall in the E-5 to E-7 pool to fill.

Filling these positions becomes a complicated affair when you consider the current distribution of ranks/grades in the Signal Company (see Figure 3). With only eight NCOs who fall into this range they will each have to take on an average of about four additional duties as the primary representative, and a similar amount as alternates.

This scenario assumes that the NCO has attended the appropriate

training and certification course to hold the positions. The training and certification process alone is enough to cripple a company considering most course durations are one week, some longer, and having to lose two NCOs to attend a week of training reduces the NCO ranks by 25 percent, thereby increasing the leader-to-led ratio, which I will explore next.

Leader-to-led Ratio

The leader-to-led ratio that the company is forced to work with is abysmal. You can better see lack of key leaders in the Signal Company in Figure 3 which shows what the company is currently authorized and how they got to this point over the past 10 years. To provide a frame of reference: according to the latest IBCT Modified Table of Organization and Equipment and Infantry Rifle Company and a Field Artillery Battery both have around a 1:3 leader-to-led ratio. This ratio can get as high as 1:4 in these organizations but only rarely and only in the case of specialty teams/squads.

Right now, the Signal company is operating at a 1:5 leader-to-led ratio in one TCN team and a 0:5 ratio in the other as there is no NCO in this TCN team. This complicates two aspects of life for this team. First, in a normal “day-to-day” environment we have one leader who is responsible for the individual task training

(Continued on page 26)



Figure 1 shows the total number of personnel authorized in the company from FY05 to FY16.

Company Additional Duties

- BOSS Program
- DFAC Representative
- Field Sanitation Team
- Unit Armorer
- Mail Clerks
- Family Care Plan Program
- Hearing Conservation Manager
- Key Control NCO
- Crime Prevention NCO
- Building Fire Marshall
- Resiliency Trainer Assistant
- CBRN Officer/NCO
- Information Assurance/Sys. Officer/NCO
- AOAP/Command Maint. NCO
- Master Driver
- Energy Conservation Officer
- Air/Rail Load Specialist
- Environmental Compliance Officer/NCO
- ARIMS Records Coordinator
- Gov't Purchase Card (GPC) Holder
- Weight Control Program
- Schools NCO
- Barracks NCO
- Command Supply Discipline Monitor
- Retention NCO
- Master Fitness Trainer
- TMDE
- Company Sponsorship NCO
- Absentee Baggage Custodian
- Army Emergency Relief
- Unit Prevention Leader
- AA&E Key Custodian
- Hazmat Officer/NCO
- Unit Movement Officer
- COMSEC Custodian
- Equal Opportunity Leader
- Physical Security Officer/NCO
- Master Resiliency Trainer
- SHARP
- Safety Officer/NCO
- Voting Assistance Officer
- Unit Claims Officer

Figure 2

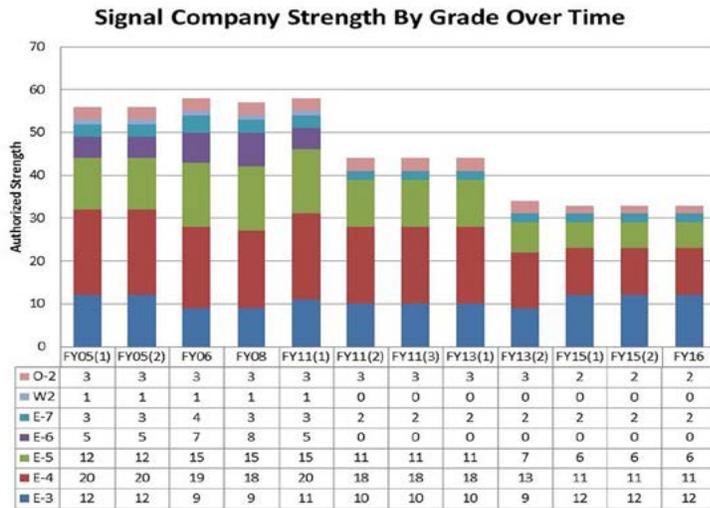


Figure 3 shows the disposition of grades in the Signal Company from FY05 to FY16. Please note O-3 and E-8 grades were removed as they remained the same throughout the sample period.

(Continued from page 25)

proficiency, administration, counseling and daily management of five or more subordinates. Similarly, the commander and first sergeant have to manage two platoons as well as two separate teams in the TCN team and SNE crew (1:4) which have no other higher organizational element.

Aside from this, the platoons themselves and all the SNE crews are operating at a much lower 1:2 ratio. Creative maneuvering of the separate TCN and SNE crew can place them under the administrative control of one of the two platoons, but this solution only solves the problem at the company level, increases the ratio at the platoon level, and does not solve the problem in the TCN team.

Equipment and Missions

Following this, there is the issue of legacy equipment which remains in the Company. The Secure Mobile Anti-jam Reliable Tactical-Terminal and the High Capacity Line of Site System have been staples of the Signal company since its inception.

Despite this, however, there are currently no personnel authorized to operate or maintain these systems. Due to the legacy nature of the SMART-T there are relatively few subject matter experts that can guide a new leader though an inventory of the equipment much less put it into operation and perform maintenance on more than the HMMWV that it is attached to.

Regarding the HCLOS, the situation is slightly better, but still fundamentally flawed.

Up until FY 2013 a five-Soldier HCLOS team existed in the company specifically to install, operate and maintain the HCLOS. After FY 2013 the Army eliminated this team but retained the equipment. While there remain trained HCLOS operators in the company in the form of 25Q Transmission System Specialists they are coming largely from the TCN teams. To put a HCLOS into operation the Company would need to sacrifice TCN operators, thus compounding the issue raised earlier about maintaining 24-hour operational capability.

Further, with the introduction of Warfighter Information Network-Tactical Increment Two the company received a Tactical Relay Tower. The significance here is there are no dedicated personnel to operate this piece of equipment in the company.

The company is forced, yet again, to either borrow from the TCN teams or SNE crews or ask for external support from the BCT or the Brigade Engineer Battalion S-6 sections.

The Possible Solutions

Here I will propose two separate courses of action that we can take to help remedy some of the problems that I have identified and described above.

The first involves mostly personnel changes in terms of MOS and Rank with a few additions to help balance the company.

The second involves dissolving the company headquarters and distributing the two platoons which support the BCT HQ to the BCT S-6 and the TCN and SNE team which support the BEB to the BEB S-6. As a baseline, Figure 4 shows a graphic depiction of the most current approved MTOE, FY16, for the Signal Company.

I want to note that common to each of these courses of action is the removal of the SMART-T and HCLOS from the company. To retain these assemblages and intend on using them would result in a much larger increase in the personnel requirement which will be difficult if not impossible to accommodate given the current defense manning requirements. The Warfighter Information Network-Tactical Increment 2 does not provide a direct replacement for the SMART-T. However, it does provide a solid line of sight

capability. Further, The Army Communicator recently published an article showing how one unit was able to use the Combat Service Support Automated Information Systems Interface system to achieve a similar operational capability to the HCLOS. These reasons, along with the maintenance and resources requirements of the HCLOS and SMART-T, are why I propose to eliminate this equipment altogether.

course of action number one.

The goal of this COA is to better organize the company to fully man all crews and shifts, improve the leader-to-led ratio and provide more NCOs to the force to handle the mandatory additional duty requirements commonplace to every company. Figure 4 provides a graphical depiction of this COA.

This first proposal involves adding eight total personnel to the authorization for a BCT net gain of five Soldiers. These additions occur in each TCN section (I will refer to the new unit as a section as opposed to a team to avoid

confusion) and SNE team by adding one additional Soldier to each. Finally, we have added two additional Soldiers to the Company Headquarters element.

For the TCN section this allows each section to operate two full 3-Soldier shifts with a Network (25N), Transmission System (25Q) and Satellite (25S) expert on each team. Further, we have added a Staff Sergeant (25N3O) position to each TCN section to manage the two teams (shifts) providing oversight, administrative assistance and mentorship to the two junior NCOs in the section. With a Staff Sergeant leading the section and a Sergeant in charge of each team we have reduced the leader-to-led ratio in the TCN sections to a manageable 1:2 at both the team and section level.

For the SNE crews we have added one more 25U1O to each SNE crew so that the company no longer has to detach from other, already short, units to fill every position in the SNE. Please note here that these positions are not a net gain for the BCT as they can come from the BCT S-6

(two positions) and the BEB S-6 (one position). Largely what this change means is that the company leadership is no longer forced to make the decision on whether to man the Gunner Seat or the SNE Operator seat, because they cannot do both with only three Soldiers in the crew. To be fair, this does increase the leader-to-led ratio from 1:2 up to 1:3, but as stated previously, a 1:3 ratio is commonplace and, arguably, ideal in the IBCT.

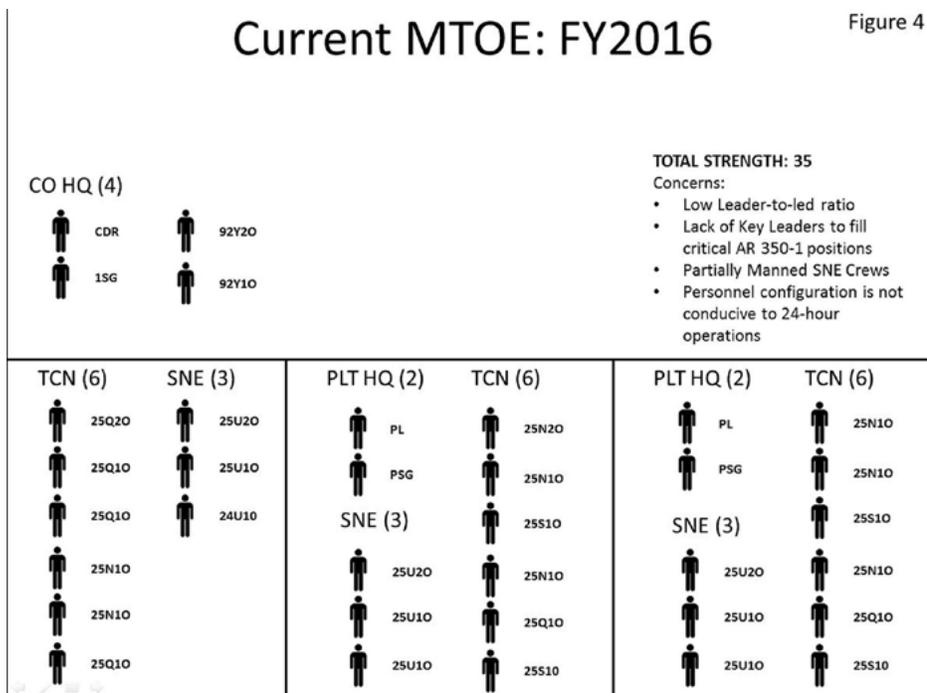
Finally, the last two additions occur at the Company Headquarters with the addition of a 25N1O and 25Q1O. The purpose of this change was to provide for flexibility in the event illness or injury causes attrition in the platoons. Further, these two operators can deploy to install and operate the TR-T as needed. This would be an ad hoc solution, but one that keeps numbers down in the organization. Additionally, these Soldiers can also function as command team drivers or an ad hoc "training room" without having to borrow from other platoons, sections or teams to fill these positions.

Overall, this course of action more added benefits. The Company remains intact as an organization and is able to provide a full complement of services to the supported BCT and BEB headquarters without reducing capacity to meet other mission requirements.

Course of Action 2

The main goal of this COA is to improve the leader-to-led ratio and fully man all sections and teams while providing the IBCT a net loss of 12 personnel authorizations.

(Continued on page 28)



(Continued from page 27)

This COA eliminates the necessity for the company to fill all additional duty positions and conduct all mandatory training on its own. However, this course of action does have far-reaching implications involving career development for 25U master sergeants, 25W4O platoon sergeants, and Signal captains; however I will offer some advice there as well. Figure 6 provides a graphical depiction of this COA.

To begin we will eliminate the company headquarters element altogether. I do this because the only reason I see that the Signal company has to manage all mandatory training and additional duties on its own is because it is a company and the only organizational aspect which makes it a company is that it has a commander, first sergeant and supply section. If we eliminate these four positions we have effectively eliminated the need for the company to manage the aforementioned requirements completely on its own.

The next portion of this course of action is similar to COA 1 in that we have improved the leader-to-led ratio and fully manned all sections and teams by increasing each TCN section and SNE team by one Soldier each and by adding two Sergeants and one staff sergeant to each TCN section. Here we will see the same benefit as in COA 1. The major change here for the TCN sections is that they will now belong to the BCT S-6 section. This relationship is good for two reasons.

First, the BCT S-6 will now have full control of the personnel and equipment in each of these platoons and no longer has to work through the BCT and BEB S-3 sections to manage their employment.

Second, the BCT S-6 has direct control over the TCN sections' and SNE crews' training proficiency. This is made easier because of the direct relationship and close proximity, but also for the fact that the training guidance and training calendar has a more direct line from the BCT to the platoons that will support it.

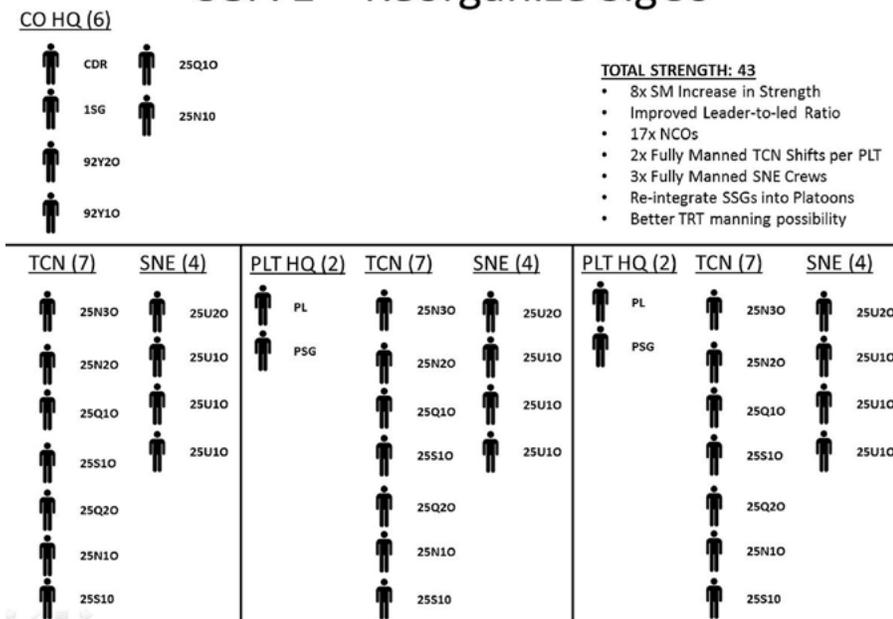
Finally, here we added a position of the Brigade Network Operations Officer and filled it with a 25A O-3. Similar in function to a Division NetOps officer, the BDE NetOps officer will be responsible to the BCT S-6 for management of the network, which now includes the two BCT nodes in close proximity. The career implication here is that this position would now have to become a key developmental position for a Signal captain since there is one less KD position in the IBCT now.

However, this is not a new concept for the Army. For instance, Military Intelligence captains have the BCT A/S-2 and S2X position which are considered KD assignments; this signifies to me that a staff position as a BCT NetOps Officer could be considered commensurate to these other BCT staff positions in terms of experience gained by the officer. Critically, we eliminated three senior NCO positions altogether; those are the company first sergeant (25U5M) and the two Platoon Sergeants (25W4O). As depicted in the graphic of this COA, I have not offered these NCOs positions in in the new BCT S-6 structure. However, I will note that the 25U5O could transfer to the Field Artillery Battalion to be the S-6 Section Chief, a position which was in years passed allocated for a 25U5O.

For the 25W4O platoon sergeants however I can offer no suitable position in the BCT structure as the BCT S-6 section is already authorized four E-7 level positions and there are no other feasible positions available in a BN S-6 or at the company/troop/battery level. Please note that I have only examined the IBCT MTOE for this paper, so there is a possibility that another type of

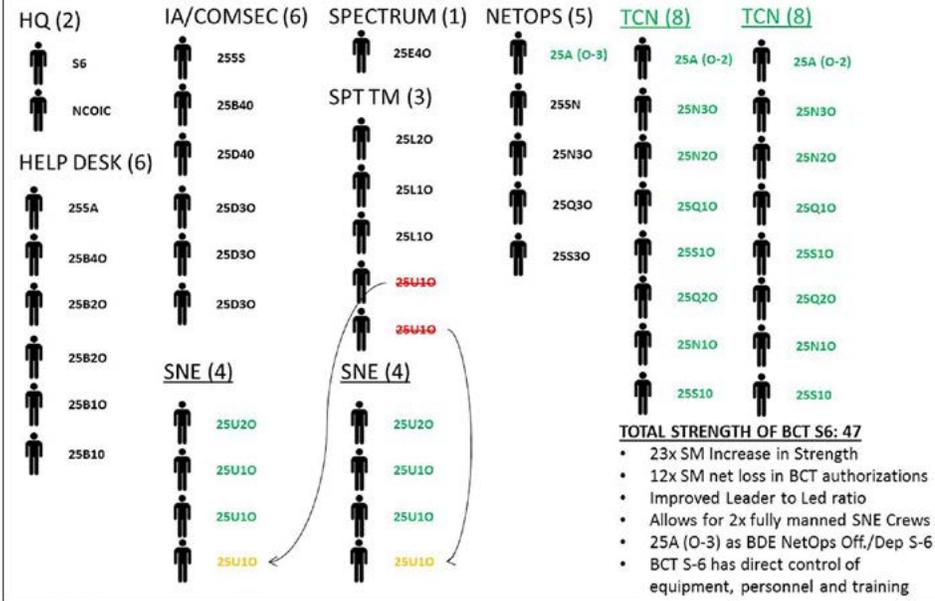
COA 1 – Reorganize SigCo

Figure 5



COA 2 – Transfer to BCT S-6

Figure 6



deployments due to less than ideal personnel authorizations. The unit is currently plagued with issues concerning authorized strength, the positioning of key leaders and an abundance of equipment that the unit is not set up to operate or maintain. Solving these issues is not a complex task.

Either of the two COAs outlined above can put these Soldiers and Leaders in a better position to train and accomplish their mission without having to make sacrifices in personnel or capabilities to do so. The IBCT has a large mission to provide C4ISR signal systems to the IBCT Headquarters which it must accomplish by operating increasingly complex systems in the most challenging and demanding environments. They are fully prepared to take on this mission, and have been for years. We owe it to these Soldiers and leaders to make their jobs a little easier by not forcing them to live in an environment that is constrained from the outset.

organization can benefit from these 25W40 positions.

I will not describe the BEB TCN section and SNE crew in detail, only to say that their organization will match COA 1 and that both entities will transfer from the Signal company to the BEB S-6 Section. This provides the same benefits to the BEB S-6 as that of the BCT S-6 albeit with one less level of coordination required.

Also of note here I would like to point out that this COA improves training and operations in that the command relationship

with the TCN sections and SNE crews because the relationship is organic and is not subject to a directed command relationship described by an operations order. Depending on the drafter of this order the directed relationship may not always best support the parent or gaining unit.

Conclusion

For too many years the IBCT Signal Company as we know it has struggled to accomplish their assigned missions in garrison, training and operational

CPT Vernon Pittman is a former company commander of C Co, 1BSTB/7BEB, 1BCT, 10th Mountain Division. He is currently serving as a deployable communications and information Systems staff officer in the NATO CIS Group in Belgium.

ACRONYM QuickScan

BEB – Brigade Engineer Battalion
CAISI - Combat Service Support Automated Information Systems Interface
C4ISR – Command, Control, Communications, Computer, Intelligence Surveillance and Reconnaissance
CBRNE – Chemical, Biological, Radiological, Nuclear and Electric
FY – Fiscal Year
HCLOS – High Capacity Line of Site

IBCT – Infantry Brigade Combat Team
MTOE – Modified Table of Organization and Equipment
NCO – Non-Commissioned Officer
SMART-T – Secure, Mobile, Anti-jam Reliable Tactical Terminal
SNE – Soldier Network Extension
TCN – Tactical Communications Node
TR-T – Tactical Relay Tower
WIN-T – Warfighter Information Network-Tactical

Lessons & Best Practices

Answers to the Test

By Scott Gorectke

The Cyber Center of Excellence Lessons and Best Practices Branch is in the business of making sure our organizations adhere to the best practices and never make the same mistakes twice.

In other words we provide the answers to the test.

The established concept of collecting observations and lessons learned from military forces has driven organization change and increased unit performance. Armies have looked internally to see how to improve their capabilities for hundreds of years. Today, many of the Centers of Excellence have this capability – to address challenges and document successes through the examination of doctrine, training, material and non-material solutions.

Constantly evolving environments of Signal, Cyber, and Electronic Warfare Operations make this a critical capability in our success as the proponent of Signal, Cyber, and Electronic Warfare in this era of technological warfare.

Accordingly, the Cyber Center of Excellence has created a provisional organization called “Lessons and Best Practices.” The Cyber Center of Excellence Lessons and Best Practices branch is comprised of a mix of military officers, warrants, enlisted, government civilians, and contractors with a combined experience of more than 275 years. Collectively, we have experts in Signal Communications, Cyberspace Operations, and Electronic Warfare Operations. Our mission is to collect, analyze, assess, and integrate Lessons and Best Practices through the doctrine, organization, training, materiel, leadership, personnel, facilities and policy process to drive continual improvement of the Army’s capability to employ Signal, Cyber, and Electronic Warfare in support of unified land operations.

Lessons and Best Practices is a resource that is always ready and available to deliver vital information and develop solutions to the challenges Soldiers face, which saves lives and ensures the continuous advancement of our technological warfare capabilities. To anyone who has participated in a Combined Training Center rotation or who has worked as an Observer-Controller/Trainer at a

Combat Training Center it is common knowledge that units will have similar challenges. Some children learned that a stove is hot by touching it, there are other children, who were told by their parents that the stove was hot, based on their own painful experience. These children chose not to test that the stove was hot and avoided the pain of getting burned. Like the latter child, Lessons and Best Practices seeks to help units leverage combined experience to learn and increase operational effectiveness.

The Cyber Center of Excellence Lesson and Best Practices branch begins the process by receiving requirements from across the Cyber Center of Excellence and in some cases from the operational force Cyber Protection Brigade or Army Cyber. We are always available to assist and to collect any information that could help address operational force requirements. Similar to a collection management process the Lessons and Best Practices branch receives and validates the requirements and then determines where to best employ our reconnaissance assets, our trained analysts. The venues that we attend include: Combat Training Centers, National Training Center, Joint Readiness Training Center and the Joint Multinational Readiness Center rotations, Army and Joint exercises, home station training, unit Umbrella Weeks (leader and staff interviews), one on one interviews with key leaders or Subject Matter Experts, partnership with industry, academia and unit visits Continental United States or deployed). While at the events we observe and document information to answer the requirements that we have been given.

Upon completion of the event the analyst is debriefed and the real work begins. The observations made are analyzed and validated based on Doctrine, Organization, Training, Materiel, Leadership, Facilities, and Policy. Through this process we attempt to ensure what we observed was not an isolated incident, only relevant to the observed unit, and confirm the observation meets one of our requirements and has value to the Cyber Center of Excellence, the force or both. During this process we also validate our observations as required with the Combat Training Centers staff or other required organizations. These observations are then analyzed against the Doctrine, Objective, Training, Materiel,

Leadership, Personnel, Facilities, and Policy model, many times in partnership with Subject Matter Experts from relevant subject areas, to identify what has to be done to address any of the observed issues.

Furthermore, observations are analyzed to determine if they indicate any trend (s) for the Army and potentially identify significant gap(s) in capability. Observed gaps are addressed through collaboration with the, appropriate Subject Matter Experts to identify potential solution(s) to any identified challenges. This is a very important step as we develop recommended solutions and make our initial determination of the cause/owner to provide a recommended solution.

The results of the analysis are then coordinated with the appropriate offices to complete the final report. The reported information can then be used internally by the Cyber Center of Excellence to apprise the development of doctrine, revision of training, material solutions development, concept, development, or other initiatives. This final report can prove to be extremely valuable to units for the development of Home Station Training plans, and or the preparation for upcoming Combat Training Center rotations or deployments. Since experience has shown us that units have very similar struggles this information could be equivalent to receiving the answer key to an upcoming test weeks or months in advance.

The strength of our process is that we are able to individually track from observation and collection through analysis, vetting, validation, and publication all observations. All final lessons learned have a unique tracking

number and can be used for future analysis, planning, and training development. The results of our analysis is provided in written reports and is warehoused on the Joint Lessons Learned Information System at <https://www.jllis.mil/apps/index.cfm>, which requires Common Access Card authentication. Our reports as well as other useful information, such as Standard Operating Procedures and articles can be located by going to the <http://cybercoe.army.mil> website and clicking the Lessons and Best Practices link, which will take you to <https://lwn.army.mil/web/ctl/home>, also requiring Common Access Card authentication.

Additionally, the Lessons and Best Practices branch produces articles like the one you are reading now, to provide information to select audiences. Not only do we want to be a resource of information on current operations, we will also provide information on emerging technology, tactics, and capabilities. Communication is the key to solving emerging issues therefore we regularly engage with Soldiers who have questions or concerns through our website or directly via phone or email. We frequently answer questions, assist in locating publications or products, and share information

to support Soldiers and leaders in any operational environment.

With the Cyber Center of Excellence Lessons and Best Practices branch as a ready resource for our Signal, Cyber, and Electronic Warfare forces there is no reason to repeat the same mistakes or challenges of past units. We encourage you to review our websites, read our reports, and reach out to our team, so that we can assist you and your unit. In addition, we are always looking for feedback on how our work can be adjusted or improved to better support Soldiers and leaders in the generating and operating forces. We are in a truly challenging operational environment and only through collective learning can we hope to keep pace with the demands of our fields. So, our gift to you is, "the answers to the test."

Scott Gorectke graduated from Augusta State University in 2011 with a degree in History. He served at Tingay Dental Clinic as a research assistant, where he received the Army Achievement Award for meritorious service. He currently serves as a publication specialist for the Cyber Center of Excellence's Lessons and Best Practices Branch.

[Join the Discussion](#)

<https://SIGKN.army.mil>



ACRONYM QuickScan

CAC - Common Access Card
CTC - Combined Training Center
CCoE - Cyber Center of Excellence
EW - Electronic Warfare
DOTMLPF-P - Doctrine, Organization, Material, Leadership, Personnel, Facilities-Policy -
HST - Home Station Training
JLLIS - Joint Lessons Learned Information System
L&BP - Lessons and Best Practices
SME - Subject Matter Expert

Stay Ready

INSTALLATION AS A DOCKING STATION

*By Scott Gorectke
LTC Chris Walls*

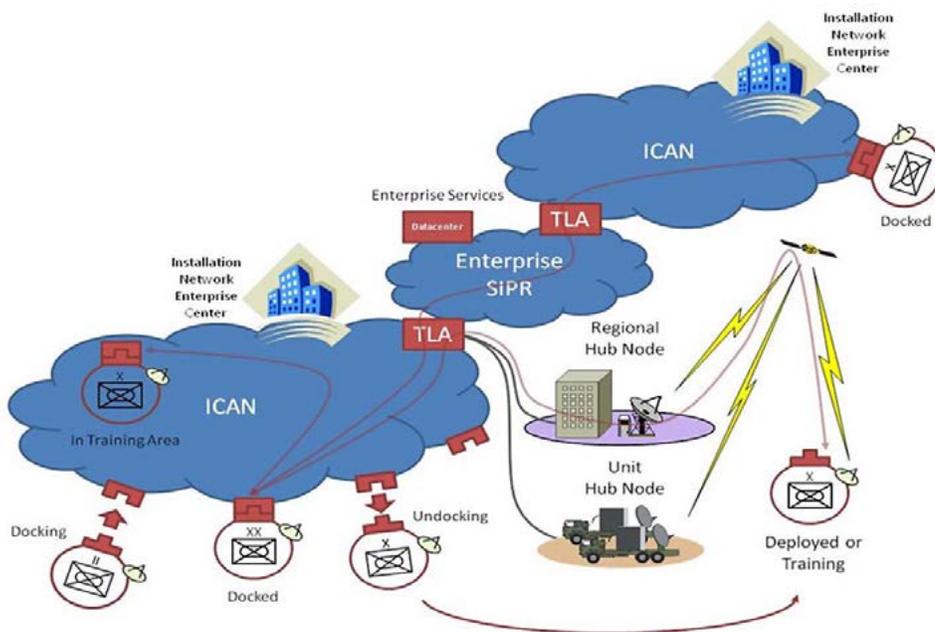
Over the last 14 years the Army has deployed the most capable network in history. As a network-centric Army, we have enabled commanders to leverage numerous capabilities simultaneously resulting in overwhelming combat power. As an Army we have done this in an uncontested environment where our adversaries have been unable to threaten the security of our networks. Those conditions will not exist in future conflicts. Our adversaries will have near peer or in some cases more advanced capabilities to threaten the

security of our networks. Units cannot arrive on the battlefield unprepared for cybersecurity on a network that they are unfamiliar with, because they only utilize it once or twice a year. This level of readiness could lead to mission failure in future conflicts.

Installation as a Docking Station is a practice makes perfect, train as you fight concept for cybersecurity. The forthcoming ATP 6-02.71 explains that “through cybersecurity, DODIN operations providers protect, monitor, analyze, detect, and respond to unauthorized activity within DOD information systems and

computer networks.” Army units are currently only responsible for conducting cybersecurity on their tactical networks while at the training centers or when deployed. When in garrison this function is provided by the NEC, it provides enterprise services to Army units. Units traditionally do not employ their tactical networks, and therefore they do not conduct cybersecurity, while in garrison. Tactical networks and the skills to operate and protect them have become increasingly more complex. One would assume that with the increase in complexity, there would be an increase in the amount of time devoted to training these tasks, but that has not been the case.

IaaS as a concept was developed in 2005 and then codified in a CONOP by the Cyber COE TRADOC Capability Manager Networks and Systems in June of 2014. IaaS provides units the ability to continuously operate and protect their networks. Under this concept units connect their tactical network through local Network Enterprise Center that provides access to either a regional hub node or unit hub node. This connectivity allows access to the WAN (internet) and/or Enterprise SIPR bringing the tactical network to life. The IaaS concept



Installation as a Docking Station Model

allows units to continuously operate their tactical networks, allowing opportunities to train, develop tactics, techniques, and procedures, and develop standard operating procedures. In addition, continuous operation of the network will ensure that networks remain patched with updated IAVA. IaaS creates the opportunity for units to train their cybersecurity workforce and address issues and training deficiencies outside of a deployment or crisis scenario in a lower threat environment. This can equal a significant increase in their combat readiness. This concept represents a paradigm shift and allows Signal Soldiers to train as they fight on their warfighting platform and to increase their technical competency.

Training on tactical systems only at a CTC will be a legacy with the implementation of IaaS. IaaS delivers additional training and flexibility due to the ability to relocate servers and clients to different locations and installations without requiring significant reconfiguration or satellite connectivity. The uniform plug and play environment enhances capabilities by providing the

necessary tools Soldiers need and the ability to go from Home Station to other tactical environments with less difficulty. IaaS provides Soldiers the opportunity to improve proficiency in individual tasks on tactical IT assets and update their respective skill sets.

Units can train daily on the collective task associated with cybersecurity such as network operations, network monitoring, scanning, penetration testing, server and configuration management, and policy enforcement. Soldiers and units would have the opportunity to develop skills in garrison, in controlled tactical environments providing them with the necessary time to develop expertise creating a more capable force.

Despite the clear benefits the units that actually have implemented IaaS are still in the minority. The primary challenge for IaaS is acceptance of the concept as a priority for mission readiness. In order to cross this hurdle IaaS will require service

level command emphasis to set the conditions with guidance and policy on the implementation of IaaS. Information on how to implement IaaS can be found at the CAC enabled 7th Signal Command's excellent website at the following URL <https://army.deps.mil/NETCOM/sites/7thSignal/ges/7thSCTacticalConnectivity.aspx>. Units that embrace the IaaS CONOP will be able to continuously operate their tactical networks and train daily on cybersecurity. The result will be a significant increase in mission readiness for future conflicts.

LTC Chris Walls joined the newly established Cyber career field in 2015 and currently serves as chief of Doctrine and Lessons Learned and Best Practices Division of the U.S. Army Cyber Center of Excellence.

Scott Gorectke graduated from Augusta State University in 2011 with a degree in History. He served at Tingay Dental Clinic as a research assistant, where he received the Army Achievement Award for meritorious service. He currently serves as a publication specialist for the Cyber Center of Excellence Lessons Learned and Best Practices Branch.

ACRONYM QuickScan

CoE - Center of Excellence
CTC - Combat Targeting Center
CONOPS - Concept of Operations
CAC - Common Access Card
IAVA - Information Assurance Vulnerability Assessment

IT - Information Technology
IaaS - Installation as a Docking Station
NEC - Network Enterprise Center
NETOPS - Network operations
SOP - Standard operating procedures
TTPs - Tactics, techniques, and procedures

McArthur's Own

Supporting a Strong Europe

*By LTC Delton Nix, Jr.
CSM Woody Carter*

In support of a Strong Europe, the 52nd Strategic Signal Battalion (MacArthur's Own) provides strategic critical command, control, and communications support to the most significant customer base in the Department of Defense. These customers include Headquarters, U.S. European Command, Headquarters, U.S. Africa Command, and many other key tenant organization in Southern Germany within the Stuttgart area of responsibility. Day in and day out, the 52nd SSB strives to produce the best Enterprise and Network Services to the Joint Warfighter.

A Unique Mission Set

In order to provide the best customer support to its significant customers, the 52nd SSB must maintain a unique mission set that is vital to the success of the major units it supports across Europe. Some of these missions include; providing secure/unsecure and voice/data information technology services, Dial Service Assistant & Dial Central Office for Defense Switched Network, a Joint Nuclear Operations Center. COMSEC account, CG Commo teams, providing force protection to a neighboring base and finally, we support U.S. Army Europe Commander's Five Pillars of Strong Europe by "Empowering Junior Leaders."

Information Technology Support to Major Customers

With numerous professionally technical DA civilians and contractors, the 52d SSB is able to provide IT support to six major customers which all have their own enclave. Across these six enclaves, there are several VIPs consisting of flag officers, general officers, senior executive service senior leaders and key principle staff officers and senior enlisted leaders. All these VIPs get priority placement when an IT issue arises and must be remediated as soon as possible. There are also NIPR and SIPR accounts that must be maintained. In addition to the normal NIPR/SIPR accounts, the battalion must maintain a Defense Red Switch Network, provide

wireless device support, manage a Campus Area Network, and provide support to Voice over IP / Voice over Secure IP telephony devices.

Dial Service Assistant and Dial Central Office for DSN

With several great local national hires, the battalion operates a 24x7 console-based DSA facility providing world-wide DSN operator assistance and support for all DOD customers in Europe.

In addition to that, the 52nd SSB operates a hub and spoke network of multi-function and end office switches providing world-wide access to non-secure voice services for DOD customers and their supporting agencies located on U.S. Army installations across Southern Germany. All this, would not be possible without our local national hires.

Defense Red Switch Network

By contracting out for support, the battalion is able to operate and maintain a 24x7 DRSN providing multi-level, secure voice, and voice conferencing capabilities to the National Command Authority, the Joint Chief of Staff, the National Military Command Center, Geographical Combatant Commanders and their command centers, warfighters other DOD agencies, government departments and NATO Allies. This DRSN facility was awarded the DISA DSRN Facility of the year for FY 14.

A Joint Nuclear Operations Center

Joining forces with Airmen in the EUCOM headquarters, the 52nd SSB has the distinct privilege of manning a Joint Nuclear Operations Center. It operates and maintains radios and satellites communications systems that provide USEUCOM with 24x7 access to U.S. and NATO Command and Control Networks. In 2013, the JNOC was recognized by the Joint Chief of Staff of the Army as having the best training program in the Army.

COMSEC Account

With tremendous DA civilians and Soldiers, the 52nd SSB is responsible for providing

communications security custodian functions for COMSEC accounts. The COMSEC Management Office has been inspected by the Network Enterprise Technology Command, the Communications Security Logistics Activity agency, by the Department of the Army Inspecting General's office and not once in the past two years have they ever failed an inspection. This, is in large part due to our DACs and their constant continuity, that CMO has been so successful.

Geographic Combatant Commander's Commo Team

The 52nd SSB supports two GCC Commo Teams. The teams provide 24/7 reliable access to voice, data and video communication support for the commander, USAFRICOM and deputy commander USEUCOM while in garrison, using a variety of communications systems and capabilities. The teams install, operate, and maintain fly away kits; for the USAFRICOM CDR and the Deputy USEUCOM. The members of these communications teams are highly trained and very proficient at providing the best communications possible to the combatant commander they support. They are constantly on the move supporting their

commander while traveling across four continents and numerous countries; they have never failed.

Force Protection

Teaming up with DISA-EUR, the 52nd SSB still does its part to keep the community safe. Members from the battalion and DISA-EUR conduct random antiterrorism measures to enhance our threat response capability. This capability rounds out how the battalion is doing its part to protect our nation against cyber threats and physical threats.

MacArthur's Own

The 52nd Strategic Signal Battalion is "MacArthur's Own." During World War II, the battalion supported General Douglas MacArthur and participated in a total of four campaigns during, Dutch New Guinea, Leyte, Luzon and the southern Philippines. It was during these campaigns that the battalion received the honor of being known as MacArthur's Own

The 52nd SSB is made up of Soldiers, DACs, contractors and German Local Nationals.

Its mission is to build, operate and defend critical communications network infrastructure and capabilities to enable Unified Action for two major Combatant Commands thru their ability to mission command assigned service component commands, multinational forces along with other key enablers supporting both Combatant Commands in their AOR.

This unit has greatly enhanced our personal and professional experience. For this unit to be so small and yet be so responsible for supporting two combatant commanders, a Joint Nuclear Operations Center and manage a COMSEC account in the Army, it amazes us. The Soldiers, DACs, contractors and Local Nationals are the best at what they do and it because of their hard work and dedication, and many others like them that we, service members across Europe, can make 30,000 look like 300,000 and maintain a strong Europe.

LTC Delton Nix, Jr. serves as the battalion commander for the 52d Signal Battalion, Stuttgart, Germany.

CSM Woody Carter currently serves as a 52nd Signal Battalion command sergeant major.

ACRONYM QuickScan

AOR - Areas of Operation
CAN - Campus Area Network
CG - Commanding General
CINC - Commander in Chief
CJTF-HOA - Combined Joint Task Force - Horn of Africa
CMO - COMSEC Management Office
COMSEC - Communications Security
DAC - Department of the Army Civilians
DAIG - Department of the Army Inspecting General's
DCO - Dial Central Office
DISA-EUR - Defense information Systems Agency - Europe
DOD - Department of Defense
DRSN - Defense Red Switch Network
DSA - Dial Service Assistant
GCC - Geographic Combatant Commander's

IT - Information Technology
JCS - Joint Chief of Staff
JNOC - Joint Nuclear Operations Center
MARFOREUR/AF - Marine Forces Europe & Africa
NCA - National Command Authority
NC2 - NATO Command and Control
NETCOM - Network Enterprise Technology Command
NMCC - National Military Command Center
SEL - Senior Enlisted Leaders
SES - Senior Executive Service
SSB - Strategic Signal Battalion
USEUCOM - United States European Command
USAFRICOM - United States Africa Command
VoIP - Voice over Internet Protocol
VoSIP - Voice over Secure Internet Protocol

2nd Signal Battalion Facilitating NATO Command and Control

By LTC John C. Hinkel, Jr.

The secretary of the Army and the secretary of defense both have stated the importance of interoperability within a multinational alliance.

While this is something that an Army Signal battalion practices on some operations and exercises, it is a routine occurrence within NATO Signal Battalions. The U.S. Army element of the 2nd NATO Signal Battalion has a unique opportunity to foster interoperability across NATO while building partner capability, which directly contributes to enhancing collective security across the alliance.

The NATO command structure contains three multinational signal battalions and a group headquarters, and the 2nd NATO Signal Battalion is the only battalion with a U.S. element. The 2nd NATO Signal Battalion is composed of members from nine nations. It is organized with a multinational battalion headquarters, six joint deployable communication modules each composed of two troops from a single nation (a DCM is roughly equal to a Signal company), and a multinational maintenance and support company. The 2nd NATO Signal Battalion commands units in three countries and maintains elements at 7-days, 10-days, and 30-days notice to move in support of an on-call NATO JTF.

“It is imperative that our leaders and organizations are capable of thriving in Joint interorganizational and multinational teams and that they seamlessly integrate multi-domain effects from air, seas, space, cyber, and land.” – Army Posture Statement 2015

“We will continue our work with allies and partners to promote regional stability and European-Atlantic integration as well as improve capacity, interoperability, and strategic access for coalition operations.” – DoD Quadrennial Defense Review 2014

The 2nd NATO Signal Battalion has a crisis mission:

On order, 2nd NATO Signal Battalion deploys to the NATO Response Force JTF’s area of operations to engineer, install, operate, and maintain deployable communication and information systems; provides C2 and logistical support to all deployable CIS (Signal) units supporting the JTF HQs and component commands in order to facilitate C2 and information flow.

The U.S. element of the 2nd NATO Signal Battalion is the most deployed U.S. Army element assigned to the U.S. Army NATO Brigade, which is the parent brigade

that exercises ADCON over all Soldiers assigned to NATO. The 2nd NATO Signal Battalion has deployed elements on many NATO operations since its activation on 1 October 2004. It deployed teams to ISAF and Resolute Support, Operation Unified Protector and Operation Active Fence supporting TBMD forces on the Turkey-Syrian border just to name some of the more recent missions. When the 2nd NATO Signal Battalions deploys it usually provides a turnkey C4I solution for the supported HQ, meaning it provides and installs 99% of the required C4I systems. The core mission of the 2nd NATO Signal Battalion is to provide deployable



Bulgarian and U.S. Signalers prepare equipment for training during a recent battalion communications exercise.

communication and information systems to deployable NATO Headquarters where the alliance requires.

The 2nd NATO Signal Battalion is one of three battalions assigned to the NATO Communication and Information Systems Group. NCISG is a unit of NATO's Allied Command Operations, more commonly referred to as SHAPE. The commander of NCISG is MG Walter Huhn (German Air Force) who is twin-posted as the SHAPE deputy chief of staff for CIS and Cyber Defense. He reports directly to Supreme Allied Commander Europe, GEN Breedlove in his NATO capacity, as he is also the Commander U.S. European Command.

NCISG units are located in 13 countries in Europe and comprise some 1500 military and civilian positions, making it the largest command in ACO. NCISG has deployed forces in three ongoing operations and deploys 900 plus personnel to operations and exercises in a typical year. NCISG's core mission is to provide deployed

communications and information systems to NATO HQs on operations and exercises wherever the alliance requires.

The 2nd NATO Signal Battalion is authorized 469 members from nine nations (United States, Italy, Bulgaria, Romania, France, Canada, Spain, Turkey, and Greece). The battalion is composed of six DCMs each consisting of a DCIS troop and a support troop, Maintenance and Support Company, and the battalion HQs. The United States and Italy each operate two DCMs while Romania and Bulgaria each operate one DCM. The DCM are authorized a Major as the NATO commander with a sergeant major as senior enlisted leader. DCMs are designed to deploy two NATO DCIS teams simultaneously- one major and one minor. Both the battalion HQ and M&S Coy are multinational units. A U.S. Army Signal Corps lieutenant colonel commands the multinational battalion with an Italian deputy commander. Most

(Continued on page 38)

(Continued from page 37)

of the battalion is co-located with 9th Wing of the Italian Air Force on Grazzanise Air Base southwest of Caserta, Italy. Romania operates a DCM outside of Bucharest, and Bulgaria operates a DCM outside Sofia. In total, the battalion contains 164 US service members (147 Army, 11 Navy, and 6 Air Force).

The practical mission of the battalion is to prepare for operations and deploy to engineer, install, operate and maintain NATO DCIS; activate and establish a Signal Support Group to provide command and control of all NATO DCIS assets in theater; manage the network; and to provide sustainment to all NATO CIS assets. The purpose is to facilitate the command and control of the JTF and to enable the internal and external flow of information to Alliance forces.

The battalion with some augmentation forms the core of a NATO JTF's Signal Support Group. The Signal Support Group is responsible for interconnecting NATO forces and extending NATO networks where required. Success requires detailed coordination with the supported JTF HQ and a solid working relationship with the JTF J6. Remember this is NATO and therefore multinational. Think on this for a moment. Imagine how different it is supporting a multinational JTF consisting of up to 28 nations with ranges in experience from minimal to substantial with wide-ranging styles of command and staff cultures. Consider the procedural differences and even the communication barriers when most members'

native tongue is a language other than American English. It is challenging but also professionally rewarding.

A DCM mission commander is one of the most challenging and professionally rewarding jobs in the battalion. A mission commander is the officer (commissioned or non-commissioned) leading a DCIS team. Depending on the DCIS team composition, the supported unit, and the complexity of the mission, the mission commander can range in rank from staff sergeant to major. For the majority of operations and exercises the mission commander is a sergeant first class. The mission commander will prepare his team, configure all DCIS for the supported HQ, and deploy. At the deployed site, the mission commander provides a turnkey C4I solution to the supported HQ by working closely with the A/N/G/J6, and in NATO this position is nearly always a senior field grade officer. Perhaps the most challenging tasks the mission commander faces is the coordination and execution of a sustainment plan for his team as every operation and exercise is unique especially considering that NATO forces do not have a standing deployable sustainment organization. By alliance doctrine, sustainment is both a national and alliance shared responsibility. Yet through critical analysis, innovation, and sometimes sheer will power the mission commander and the battalion staff arrive at a just-in-time sustainment plan executed in a multinational fashion. Operating daily in a multinational environment, mission commanders exhibiting

military and technical professionalism are crucial for the battalion's success.

In the past two years, the battalion has successfully deployed on numerous operations and exercises across Europe and South West Asia. The battalion maintains a major point of presence in Afghanistan supporting Operation Resolute Support as a service manager and until just recently a small point of presence on the Turkish-Syrian border. The battalion has supported exercises across Europe from Steadfast Cobalt'14 in Kaunas Lithuania to Steadfast Illusion'14 in Beja Portugal and from Trident Jaguar' 15 in Stavanger Norway to Trident Joust'15 in Transylvania Romania and Sofia Bulgaria. The battalion has mastered air-land-sea movement and routinely deploys in excess of 1000 kilometers from its peacetime locations to provide a turnkey C4I solution for the alliance wherever it is required.

So why is this important?

It sounds much like many other Signal battalion missions.

The 2nd NATO Signal Battalion is at the cutting edge of practical near-term interoperability solutions because it is a challenge that the battalion faces in every exercise and operation.

Every NATO exercise is multinational by nature and requires the rapid instantiation of NATO and national networks. It is important work as noted by LTG Ben Hodges, commander U.S. Army Europe, and former commander NATO Land Component Command who stated, "If there is a crisis anywhere in Europe, American

Soldiers will be fighting alongside allies. We'll be mixed together." He also stated, "The goal is to get Afghanistan-level interoperability without Afghanistan-level prep time."

LTG Mark Bowman, Joint Staff J6, said, "We need them (mission partners) to show up with their kit and plug in." Of course, the U.S. solution to this is the Joint Information Environment and the Mission Partner Environment at the tactical level.

However, NATO and all 28 alliance nations have recognized the same need and have developed the Federated Mission Network and a practical application called the Mission Secret network with a Mission Information Room.

Incidentally, both MPE and FMN are born from the experiences and objectives of the Afghanistan Mission Network. How does this relate to 2nd NATO Signal Battalion?

For the past year, 2nd NATO Signal Battalion, NATO CIS Group and others have conducted a series of exercises that implemented, tested, and validated aspects of FMN and the MIR.

Specifically, NATO exercise Steadfast Cobalt 15 saw the largest collection of allied signal units and headquarters implementing and testing interoperability in many years. Exercise Trident Joust15 witnessed the first operational deployment and migration of the Mission Secret MIR from a static NATO 4-star HQ to a forward deployed JTF HQ supported primarily by 2nd NATO Signal Battalion.

Later NATO exercise Trident Juncture 15 experienced the largest NATO Command Post Exercise in decades supported by every element in the NATO CIS Group and national Signal units.

Similar to MPE, FMN provides the architectural standards that allow national units and systems to connect to NATO networks to exchange information. The U.S. elements of 2nd NATO Signal Battalion are optimally positioned to facilitate the objectives of both FMN and MPE.

The 2nd NATO Signal Battalion operates in a challenging multinational environment providing turnkey C4I solutions to NATO deployed HQ. The battalion's core mission is to provide the alliance and its partners with deployed communication and information systems support wherever it is required. The battalion accomplishes its mission by employing small joint, multinational teams led by professional military and technical mission commanders deployed across NATO's operational footprint. The battalion maintains DCIS teams on short notice-to-move timelines in support of NATO crisis response operations. Like other signal units, interoperability is a challenge, but the battalion has unique opportunities to employ and test practical solutions on NATO networks with alliance partners. As the U.S. element of the battalion accomplishes these tasks, they contribute in small steps towards building partner capacity, enhancing interoperability, and deterring aggression.

LTC John C. Hinkel, Jr. is the commander of 2nd NATO Signal Battalion. LTC Hinkel entered active duty as a distinguished military graduate from the University of Akron in 1992. He is a graduate of the Armor Officer Basic and Signal Officer Advanced Courses, Command and General Staff College, Joint and Combined Warfighting School, and the Joint C4I Staff Officer Course.

ACRONYM QuickScan

ACO- Allied Command Operations
C2 - Command and Control
CIS - Communication and Information Systems
C4I - Command, Control, Communications, Computers, and Intelligence
DCIS - Deployed Communication and Information Systems

DCM - Deployed Communication Module
FMN - Federated Mission Network
HQ - Headquarters
ISAF - International Security Assistance Force
JTF - Joint Task Force
MIR - Mission Information Room
MPE - Mission Partner Environment
M&S Coy - Maintenance and Support

Company
NATO - North Atlantic Treaty Organization
NCISG - NATO Communication and Information Systems Group
SHAPE - Supreme Headquarters Allied Powers Europe
TBMD - Theater Ballistic Missile Defense

Tactical Mission Command in a Robust Multi-National Operating Environment

By 1LT Jeremiah J. Snyder

Part of the Signal Corps Branch function is to “Integrate tactical, strategic and sustaining base communications, information processing and management systems into a seamless global information grid that provides mission command systems integration for Army, joint and coalition operations ” according to DA PAM 600-3.

Throughout Operation Enduring Freedom, U.S. forces have operated with partnered nations, and thus as mission command subject matter experts, we are responsible for ensuring that our commanders have command and control of the battlefield even when the units they fall under or operate with may be not be American.

This poses many challenges, particularly to Signal officers constructing comprehensive mounted and dismounted PACE plans.

With the official end of Operation Enduring Freedom and the subsequent end of combat operations in Afghanistan, many Soldiers and leaders may no longer be planning for deployments to, or investigating recent lessons learned from the current operations in that country.

Although human nature may tend to look forward to “The next big thing,” history tells us that we must stay in

When I first arrived in Kabul, I realized that one of the primary hurdles was how all of the co-located units in Kabul--Danish, German, Mongolian, Italian, Norwegian, U.S. and UK, would communicate with each other fulfilling the very important and sometimes dangerous mission, of advising and assisting Afghan military and civilian leaders nationwide.

the mindset of completing the mission to standard before completely shifting focus elsewhere. As leaders, we need to remember that there are still many lessons and skills we can learn from the mission set that we have in Operation Freedom Sentinel that will assist our Army in future operations, whether in Afghanistan or elsewhere.

While Operation Freedom Sentinel may not have the offensive operations that often times characterized Operation Enduring Freedom, U.S. forces across Afghanistan still continue a very important and sometimes dangerous mission, that of “Advising and Assisting” Afghan military and civilian leaders nationwide.

Specifically Kabul, with its cluster of military bases, has proven to require most movements to be tactical in nature due to various threats.

On any given day, U.S. Soldiers and our allies can be seen escorting military and civilian leaders, primarily from NATO countries, across the city to important meetings and planning sessions, with weekly totals of these movements numbering well in the hundreds.

From a mission command perspective, allowing commanders of these joint missions to have situational awareness of their elements moving around the city is as important as it has ever been.

When I first arrived in Kabul, I realized that one of the primary hurdles was how all of the co-located units in Kabul--Danish, German, Mongolian, Italian, Norwegian, U.S. and UK would communicate with each other. For instance, the UK’s forces, including their Quick Reaction Force, were equipped with Bowman Radios, while the



(Photo by 1LT Jeremiah Snyder)

Part of the communications solution in the multinational operations environment of Afghanistan includes regular flights over Kabul to maintain UK Retransmission Sites, from a UK "Puma" rotary winged aircraft.

U. S. Soldiers used SINCGARS, both FM yet unable to directly communicate.

To talk to each other, a temporary solution was put in place where the UK's forces would use the radios they typically use for TACSAT, the AN/PRC 117G, and operate on FM to talk to US Forces.

This hurdle forced us to answer a question that had been around for quite some time, "what is the most effective, secure, and logical way for a multinational force to communicate in a highly volatile non-combat environment?"

It would seem that as mission command has always and forever will be a large planning consideration for every military exercise, that this should have been one of the initial planning considerations of operations in Kabul.

NATO commanders took the lead of the International Security Assistance Force Mission in Kabul in August 2003, and the initial SOP could have been for a secure, reliable radio system to be used across the Kabul Area of Operations.

There are two primary challenges to this course of action. Kabul being a large city, of over 3 million people and spanning well over 100 square miles, would require a large coverage "bubble" covering both mounted and dismounted communications. Also, the different communications platforms that some of these nations utilize (ex. Bowman vs SINCGARS) which has been referenced previously. These challenges could have been mitigated by setting up retransmission sites at a few

(Continued on page 42)

(Continued from page 41)

of the bases in the city, either those owned by the U.S. or partnered NATO nations, and by immediately establishing a standardized radio, much as the 7.62 and 5.56 rounds are standards in NATO. The planning and execution required to put all of this in place, and the cooperation level involved between the U.S. Signal Soldiers and their NATO counterparts would need to be quite in depth but by no means unnecessarily complicated.

When I arrived in Kabul, the beginning stages of actually implementing this solution were being put into place.

Cooperation between the Joint U.S./UK Signal Section had determined upon a way to get all tactical communications onto the same radio system.

The initial choices of communication had been the EADS radio, which is a small handheld radio with low level encryption, similar to the EF Johnson radio commonly used by U.S. forces, or when acceptable, a cellular phone. Since there are repeaters set up throughout the city for the EADS radios, these were a natural choice from a

convenience perspective. The end goal however, was to use the AN/PRC 152 and make that the standard NATO radio system. These radios provide more durability and better security of communication and therefore are more conducive to operations in an urban environment.

At this time, New Kabul Compound's J6 Section is still working towards this desired end state, and is making great strides towards its implementation. Retransmission sites around the city have been identified, and equipment has been emplaced and successfully tested.

A standard radio platform has also been identified and the acquisition process is well underway. Both of these took some time to plan and coordinate, but are proving to be tremendously fruitful undertakings. The UK forces testing the retransmission sites have found that these allowed communication throughout the city back to Higher Headquarters and also when on the outskirts, just as planned. The second part of this plan, the issuing of a NATO standard radio system to the U.S. and all NATO forces operating in the area, will guarantee seamless

communication while inside the "bubble."

One of the beauties of this endeavor has been learning how to avoid repeating this situation in the future. With a few key planning considerations, a multinational mission can have an established standard communications platform to provide effective Command and Control across the Battlespace. As the scenario in Kabul has shown us, this will require the early emplacement of retransmissions sites across the AO that are both well secured, and easily accessible for servicing. It also will require a standard communications platform for all partnered nations, but both of these, if successfully implemented, will pay dividends towards guaranteeing effective communications and therein helping to ensure mission success.

1LT Jeremiah J. Snyder serves as a battalion Signal officer for the 2-15th Field Artillery Battalion, 2nd Brigade Combat Team, 10th Mountain Division, Light Infantry. He also serves as the deputy officer in charge a combined U.S. and UK Signal section in North Kabul Compound, Afghanistan.

ACRONYM QuickScan

AO - Area of Operations

AN/PRC - Army Navy/ Portable Radio Configuration

EADS - European Aeronautic Defence and Space Company

FM - Frequency Modulation

NATO - North Atlantic Treaty Organization

NKC - New Kabul Compound

PACE - Primary, Alternate, Contingency, Emergency

SOP - Standard Operating Procedure

TACSAT - Tactical Satellite

UK - United Kingdom

SIGNALEERS AT WORK



SFC Paul Pearman checks SATCOM configurations on the Satellite Transportable Terminal while setting up communications at Kamp Desa Pahlawan.



(Photo by SGT Kimberly Hackbarth)

Airman 1st Class Paul Nguyen, a Tactical Air Control Party specialist with 5th Air Support Operations Squadron, sets up a SATCOM antenna on an observation point. Soldiers of 4th Stryker Brigade Combat Team, 2nd Infantry Division, worked alongside airmen from 5th Air Support Operations Squadron during a Joint Air Attack Team mission to destroy a simulated insurgent training camp northwest of Forward Operating Base Seattle at the National Training Center.

Team Building in the U.S. Army

By MAJ Cheryl L. Gray

As a leader in the military, with the current operational tempo, and relentless mission requirements, it is often difficult to take the time out to build solid, efficient, cohesive teams. The lack of time and reluctance to take that time contribute significantly to the inability to realize the efficiency that comes from a cohesive team. As leaders, we must take the time to do a few key things to improve our teams. Respect, realization of talent, willingness to accept ideas other than our own, and the ability to delegate are critical factors in building teams in the Army.

Many new Soldiers have diverse backgrounds and experiences, and bring a lot to the table that can benefit the team as a whole. Taking the time to listen to and incorporate their ideas inspires the Soldier of all ages to take ownership.

For many years young and inexperienced Soldiers, have been “beaten down” by their leaders.

They come into the Army with good ideas and intentions to make a difference yet are shut down by leaders who have a directed mission they must accomplish within a much abbreviated time frame. The Soldier has an idea that may streamline a job, but is ignored because they are new and or not forthright enough to push their idea on their leader.

This Soldier may attempt to have himself heard and be repeatedly pushed to the side as if his/her idea couldn't possibly have an effect on the outcome of the mission at hand.

Eventually, this Soldier learns that his opinion does not matter and the Army “goes rolling along” despite his input. His level of interest and personal investment wanes with time.

The result is a perfectly good, intelligent, well-intentioned Soldier sitting back and no longer offering input that may have been key to streamlining the process of whatever mission was being executed.

The key to successfully drawing this Soldier in is to stop long enough to listen to the new Soldier's input and attempt to incorporate that Soldier's ideas into the task.

In the very least, the different idea warrants a discussion and analysis before blindly being tossed aside. If even part of the idea is used, the Soldier will feel they have contributed and will feel a sense of ownership.

This sense of ownership will likely motivate the Soldier to invest more energy in order to prove that his contribution has value, thus when extrapolated across the Army, the Army in its entirety has the potential to improve. Not only will it motivate that Soldier but just as “one bad apple will spoil the whole barrel”, one good apple has the potential to be infectious to the team as a whole. Once one Soldier sees the fruits of their labor realized, there will likely be “buy-in” from more Soldiers on the team.

Another essential element of team building that contributes to the success of a team is treating all Soldiers with respect at all levels regardless of rank, age, experience, background, or education level.

When new Soldiers are brought into a team and shown that their opinion has value and that they are respected, they are emboldened to contribute more. A Soldier, who is disregarded simply because of rank, will demonstrate tendencies of someone who has been pigeonholed. That person will step back and say, “Well it doesn't matter what I do, they are going to treat me as a private, so I may as well act like one.” That individual will perform at the level of what is expected of the current rank.

In addition to listening to the Soldier, use of a respectful tone and body language goes a long way toward making that member feel part of the team. Respectful communication on all levels both verbally and nonverbally, and supportive interpersonal relationships have been consistently linked with positive attitudes toward the work environment, which leads to job satisfaction, improved job performance, and an increase in retention.

Identifying talent, intelligence and skills, then capitalizing on them are key to a good team as well. A staff sergeant was labeled as the “angry NCO.” He was a young infantryman with several deployments and a lot of residual anger. In addition to multiple deployments where he lost close friends, he had a knee injury that took him out of the field and put him in a brigade S3 staff position. He was placed at a desk and not given anything to do. He sat around, did very little,

SPC Jarvis Bunch, a Signal support systems specialist (25U) works on servers in the Information Assurance area of the IID Headquarters.



and exuded anger and discontent. After several months of the angry NCO stirring discontent, he was given a position in a section short of personnel. Despite his attitude, he was needed for a job. The supervisor recognized that despite his anger and insolence, he was intelligent and organized so he was given the job of assisting the supervisor in scheduling and tracking the hourly training and coordination of over 4,000 deploying Soldiers.

Within weeks, he had completely re-designed all of the tracking processes and increased the efficiency of the position. He took charge of the scheduling, his personality and demeanor improved remarkably, and he became a valued, productive member of the team.

The leader recognized a talent the Soldier possessed, exploited it, and ended up with a happier, more productive, efficient team member.

Allowing Soldiers to make decisions as well as mistakes is essential to building productive members of a team. Encouraging them to use their brains and be responsible for their decisions enhances ownership.

When Soldiers are forced to work under a micromanager,

it kills their drive and forward momentum. They lose the desire to make their own decisions. They lose a sense of ownership and become the equivalent to automatons. Because they have a desire to do a good job, they will continue to work and do as they are told, however they will not be as efficient, productive, inventive, or happy as if they were allowed to establish their own processes and make their own decisions. A section was taken over by a new leader. Prior to the new supervisor's arrival, the team worked for a micromanager who did not allow his Soldiers and warrant officers to make any decisions. They were told that the supervisor was the only one capable of making decisions and therefore the only one allowed to do so. This resulted in an inefficient section. The Soldiers brought their issues to their supervisor and then because the supervisor was so deeply engaged in every aspect of their section, they often ended up waiting days for the supervisor to get around to making a decision and providing them with guidance. In many cases, suspenses were missed and the team was seen as being inept and lazy by the other sections in the brigade.

Eventually the section received a new supervisor whose leadership style was more delegating in nature. The Soldiers and warrant officers were given the latitude to come up with ideas, develop solutions, and make decisions. Though it took over a month for them to re-start the process of thinking for themselves, they became a highly productive, efficient team that quickly rose to the top within the brigade and division.

Giving the Soldiers the opportunity to take ownership and make decisions lead to an influx of new ideas and efficiencies. Eventually the team began to improve efficiencies outside of their brigade by suggesting ideas that streamlined the processes in other brigades and in the division headquarters.

Allowing team members to make decisions, identifying and exploiting individual strengths, treating Soldiers with respect, and valuing ideas regardless of rank are all critical factors in building efficient, cohesive teams in the Army. Without these, teams will continue to exist, but will not realize their potential and will remain inefficient and ineffective.

Army leaders at all levels must continue to take the necessary time to build these solid, cohesive teams. Though there are a multitude of different types of leaders in the Army, many of them currently use the tools that have been discussed in this article to create organizational environments that develop young Soldiers into great leaders.

MAJ Cheryl L. Gray is currently serving as the ACofS, G6 of 1st Infantry Division, Fort Riley, Kansas.

Supporting Mission Command for Pacific Pathways: Malaysia

By CPT John Geracitano

As part of the Army's new initiative to rebalance to the Pacific region, 1-17 Infantry Battalion (Buffalos), 2-2 Stryker Brigade Combat Team based out of JBLM, Wash., deployed in September to Malaysia in support of Pacific Pathways.

The Buffalos joined the 5th Royal Ranger Regiment (Headhunters) to form Task Force Buffalo-Headhunter, participating in the Malaysian Army's annual Keris Strike exercise from 13-26 September. Together, both armies shared Tactics, Techniques and Procedures from jungle operations to maintenance procedures, while becoming immersed in the diverse and unique Malaysian culture.

Key to our success during Keris Strike was quickly establishing our ability to communicate with all echelons, attachments and foreign counterparts.

Building on the confidence from our June rotation at the National Training Center that stressed our Lower and Upper Tactical Internet, we deployed ready to operate in any environment. This confidence remained strong after encountering numerous challenges brought on by the dense jungle terrain as well as operating in a new hemisphere for the first time.

Prior to equipment load-out we installed the Ka-Band kit on the Satellite Transportable Terminal



SPC Danny Ngin of 3-25th General Support Aviation Battalion monitors FM and TACSAT radio nets on a Hard Crew Access Unit during the Task Force COMMEX for Operation Keris Strike, Malaysia.

but were unable to conduct a validation exercise at JBLM due to our location in the Western Hemisphere. Additionally, our inability to perform network recovery operations due to rapid equipment turnaround post-NTC contributed to the delay in establishing Upper TI connectivity. The Command Post Node firewall settings that successfully protected us from the Cyber Red Team needed to be restored to default. SPC Kong Lee, our LAN Manager, devoted many hours of troubleshooting to revert these settings and allow the appropriate inbound traffic. Allocating enough time between a CTC rotation and deployment pack-out would allow for proper network recovery

To assist the Buffalos with

initial setup, PACOM provided Blue Force Tracker, STT and IT Radio Logistics Assistance Representatives. These representatives proved to be essential to our communications success. Our BFT LAR, updated all BFT2 Transceivers in country and installed the necessary maps for Malaysia and Japan. The use of BFT2 and its beyond line of site features were essential in getting the message through when line-of-sight communications were degraded.

However, having an additional BFT TOC kit in the TOC for logistical tracking and coordination would be extremely beneficial.

At NTC we used Route Planning Kits to extend BFTs into

the TOC from a vehicular platform parked adjacent to the TOC. This method is feasible and expedient, but it also takes vehicles out of the fight. Overall, BFT has proved to be essential for effective mission command at all echelons.

The designated satellite for integrated waveform satellite communications presented a unique challenge. The satellite was positioned at such a low elevation that aircraft and units not located with a clear view of the horizon were unable to establish a usable connection. SFC Paul Pearman, S6 NCOIC, worked tirelessly coordinating with our sister battalion in Indonesia and 3-25th General Support Aviation Battalion to find a satellite we both could lock on in order to establish tactical satellite communication. We recommend that the headquarter element for Pathways should de-conflict satellite access authorizations based on where each unit will be located throughout the Pacific.

To close the gap in FM coverage created by distance and the jungle environment, the Buffalos implemented a previously unused capability-Extended Voice Communications. EVC allowed LOS FM communications to be relayed over the Upper TI, enabling units to use assigned LOS frequencies to communicate Beyond Line-of-Sight.

This BLOS capability was also accomplished by configuring a radio relay through the enhanced Micro Central Switching Unit to retransmit voice communications from LOS systems, through the SATCOM radios, and back to the distant end LOS systems, significantly increasing real-time situational awareness for leaders on the ground. Brigades can take advantage of the EVC and eMCSU

BLOS capability for any training/mission set. We recommend configuring all Command Post Platforms across the Brigade at home-station prior to beginning any operation to maximize potential network extension.

Task Force Buffalo-Headhunter had the privilege of operating in a joint environment with 3-25th GSAB, 585th Engineers, 81st BSTB, 2d BSB, an Air Force Staff Weather Office and Pararescue Jumpers. Deploying elements arrived with conflicting COMSEC information and satellite access authorization data, further compounding the need to establish mission command quickly.

It was immediately apparent that operating in a joint environment required coordination between communications sections at every echelon. Task Force Buffalo hosted a communications exercise to validate PACE plans and to ensure interoperability at every echelon with every system. Malaysian counterparts observed

our maneuver company during this exercise, with each Army sharing their best practices with communications equipment.

If your unit is slated to deploy on a Pathways mission, try to coordinate in advance with all counterparts to resolve COMSEC issues before hitting the ground.

Having a more compact and transportable Upper TI system is a capability gap that has emerged from this initial Pathways deployment.

The Army's new focus on creating a rapidly deployable, self-sufficient ground force has created the need for a mobile Mission Command package; something that would have been beneficial during this current Pathways rotation. Often referred to as "Flyaway Kits," these suitcase-sized systems can contain a laptop, VTC suite, telephony, and NIPR/SIPR connectivity.

Such kits are used heavily

(Continued on page 48)



Malaysian counterparts observed how we conduct communications checks and learned about our capabilities inside a Stryker vehicle during the Task Force COMMEX for Operation Keris Strike.

(Continued from page 47)

today by Special Operations and First Responder services during Humanitarian Aid and Disaster Relief operations. Because units on Pacific Pathways deployments must be prepared to conduct HA/DR missions, each BN regionally aligned with the Pacific (and

Africa) should be authorized at least two Flyaway-type kits to maintain Mission Command and self-sufficiency. As the Army returns to a more expeditionary force, we will not have the luxury of waiting for our Mission Command systems to be shipped or flown to the troops on the ground. The Buffalos were without

ABCS equipment for three weeks as it traveled across the Pacific to Japan. This is a significant amount of time considering we are only on a three month rotation.

Operation Keris Strike has greatly improved and developed the capability of the Buffalo S6 section. Our unique mission set and environment presented many new challenges, forcing us to resolve issues organically through persistence and collaboration. Sincere thanks go to all of our counterparts, U.S. and Malaysian, as well as the LARs for sharing their technical expertise and field experience with our Soldiers. We hope that this article has shed some light on planning factors to consider and lessons learned for service on a Pacific Pathways deployment.



CPT John Geracitano assists a radio telephone operator during the Task Force COMMEX on the Blue Force Tracker Tactical Operations Center Kit at the 1-17 IN BN TOC at Kamp Desa Pahlawan.

CPT John Geracitano is the technical branch chief for the Joint Deployable Analysis Team, Joint Staff, J6. Previously, he served as the S6 OIC for the 1-17th Infantry BN, 2-2 SBCT, Signal company commander for the 16th Combat Aviation Brigade, and served in numerous positions as an Armor officer with the 3d Armored Cavalry Regiment.

ACRONYM QuickScan

ABCS - Army Battle Command System
BFT2- Blue Force Tracker version 2
BLOS - Beyond Line-of-Sight
BSB- Brigade Support Battalion
BSTB- Brigade Special Troops Battalion
COMMEX- Communications Exercise
COMSEC- Communications Security
CPN- Command Post Node
CPP- Command Post Platform

CTC - Combat Training Center
eMCSU - enhanced Micro Central Switching Unit
EVC - Extended Voice Communications
FM - Frequency Modulation
GSAB - General Support Aviation Battalion
HA/DR- Humanitarian Aid / Disaster Relief
IW- Integrated Waveform
JBLM- Joint Base Lewis-McChord
LAN- Local Area Network



Digital Systems

The Broken Interoperability Link

Interoperability is a vital aspect of each training rotation at Joint Multinational Readiness Center. Command and control digital systems are intended to promote interoperability.

However, limitations and constraints, such as funding, acquisitions and cross-capability on C2 digital systems ultimately degrade and inhibit information flow between allies.

Considering these setbacks, digital systems are poor candidates for facilitating multinational interoperability.

By CPT Brittany Coughran

(Continued from page 49)

At the Joint Multinational Readiness Center, multinational brigades from all over the world join in large-scale, tactical training events designed to enhance capabilities and strengthen alliances between NATO countries. Interoperability is defined in the NATO Allied Tactical Publication-3.2.2 Command and Control of Allied Forces (February 2009) as “the ability of NATO forces, and when appropriate, the forces of partner and other nations to train, exercise, and operate effectively together, in the execution of assigned missions and tasks.”

It further defines Command and Control Interoperability as “the degree to which different forces, including forces from different nations, within NATO can work together in the planning and execution of combined and/or joint operations across the spectrum of conflict.

Effective C2 interoperability, at all levels, requires common, or commonly understood, C2 doctrine and procedures and the timely exchange of all relevant information to ensure unity of effort within the philosophy of decentralized command, and full integration and coordination of NATO forces in support of commander joint force’s missions” (NATO ATP-3.2.2, 2009, section 1-12). Interoperability is a vital aspect of each training rotation at JMRC. C2 digital systems are intended to promote interoperability; however, limitations and constraints, such as funding, acquisitions and cross-capability on C2 digital systems ultimately degrade and inhibit

information flow between allies. Considering these setbacks, digital systems are poor candidates for facilitating multinational interoperability. Using Observer-Controller/Trainer observations from past JMRC rotations and evidence gathered from JMRC Exercise Combined Resolve V, this paper will discuss the limited communications assets and capabilities within multinational taskforces.

It will also discuss communications security and intelligence sharing that hinder digital systems’ capabilities as well as diverse cultural differences between allies that constrain C2 interoperability. Understanding the constraints on C2, as it supports interoperability, is paramount towards developing multinational units at the brigade level and below, and units seeking to capitalize interoperability should invest more attention in outfitting and training liaison packages in order to bridge deficiencies in digital systems.

Command and control is defined by the U.S. Army as “the exercise of authority and direction by a properly designated commander over assigned and attached forces in the accomplishment of a mission” (Army Doctrinal Reference Publication 1-02, Terms and Military Symbols, February 2008, p. 1-8). A commander cannot exercise proper C2 without fulling exploiting all available systems, which includes personnel, regulations, assets available, standard operating procedures, and digital systems.

A multinational taskforce with optimal interoperability seeks to interweave different C2 systems



across the organization in order to enhance C2 for the commander.

Digital systems are often thought to be the most efficient form of interoperability for a taskforce: if all systems can “talk” to all other systems, then C2 is fully integrated with all C2 systems. Due to the lack of uniformity in digital systems across the NATO alliance other methods must be developed in order to best achieve desired results.

Within the NATO alliance, militaries from each of the 28 NATO nations are outfitted with different Tactical Operations Center equipment capabilities. Often these systems are limited, lack digital capability, or are incompatible with other allied nations. The interoperable “cross-talk” between these systems is rarely achievable: the networks simply do not coexist or do not have the same classification levels. Furthermore, the data is in multiple languages that other allies do not understand. During the JMRC training rotation Allied Spirit II a mechanized Infantry battalion from the Czech Republic, was attached to a Czech brigade headquarters with battalions from different allied nations, and utilized a digital C2 node called

OTS to develop and execute battle staff functions. While this digital capability appeared advantageous for achieving interoperability, it actually hindered the overall interoperability with adjacent battalions. While the Task Force and its brigade headquarters had access to OTS, other units in the multinational brigade did not. Information from the Task Force to its parent Brigade through digital channels did not reach adjacent battalions. During Exercise Swift Response 15, multinational battalions fell under the command of the 1st Brigade, 82nd Airborne Division. Comparing the Airborne German Battalion's TOC, task organized with German, Dutch and Polish companies, and the Czech Republic Task Force the C2 systems were drastically different: one had no digital

network at all, utilized obsolete radio platforms from previous decades, and relied primarily on analog battle tracking systems. Despite being provided a coalition network that linked them digitally to the brigade headquarters, the battalion staff relied primarily on their own analog tracking systems which made it difficult to share information between sister-battalions and their higher headquarters. The common operating picture, current situation report, and up-to-date battle tracking were confined to map boards within the TOC. The Coalition Network digital systems were used only by U.S. liaison Soldiers allocated to the battalion from the brigade headquarters. In addition, the radios that each company used were incapable of using common classifications and encryption

types of communications security, so the only way to achieve radio communication between the German, Dutch and Polish companies was with single-channel, plain text FM communications.

During JMRC exercise Combined Resolve V, similar systems were employed by a Romanian battalion that was task organized with Georgian, Bulgarian, Romanian and Albanian companies. The battalion had no digital network. Instead, they relied on the training network provided by JMRC called "coalition network" as well as very high frequency and high frequency radio communications. Incompatible communications systems within the battalion

(Continued on page 52)



Lithuanian Special Operations soldiers apply training they have received from current U.S. Joint Terminal Attack Controllers at the Joint Multinational Readiness Center as they practice using advanced simulations equipment where they can conduct full missions prior to executing the tactics in the field. JTAC Soldiers execute complex air-to-ground missions that integrate ground-based radio operations with fixed and rotary wing aircraft in combat environments. The training they receive at JMRC with its advanced simulations and real life squad tactics lanes prepare them for real combat scenarios.

(Continued from page 51)

constrained C2 interoperability. A program defined as Multilateral Interoperability Program has been implemented in some nations to establish interoperable communications amongst the different platforms, but its success has been marginal.

It is intended to connect different C2 systems from different nations so data and information can be shared, regardless of the interface. In order for the MIP to work properly, each nation must properly configure their own digital gateways and systems to communicate with the distant-end MIP.

The MIP, while endorsed by NATO, is not a NATO program, so not all NATO allies participate. As of October 2014, France, Germany, Romania, Great Britain, and Poland are running MIP 2.0 or 3.0. The U.S. and other militaries have upgraded to 3.1, which is incompatible with previous versions (JMRC Mission Command and Simulation. "What is MIP?" PowerPoint Presentation, 26 Oct 2014). The MIP, if executed properly, could solve part of the

digital interoperability problem, but currently it has had minimal impact.

In addition to the different MIP gateways, each nation has its own communications security and intelligence sharing procedures that limit information accessibility. In some cases, even if C2 interoperability is achievable (as is the case with some tactical radio communications), many nations lack the necessary cryptography or the understanding of how to acquire it. This is likely a third order effect of intelligence regulating and national security. As a result, it is far more common for multinational units training at JMRC to use single channel, plain text voice communications.

The cultural differences observed between the units conducting unilateral operations is another challenge in achieving C2 interoperability. A lack of unity and shared identity at the Battalion and Brigade level stovepipes information flow while language and cultural barriers constrains communication. During Exercise Combined Resolve V, OCTs observed that information flowed downward

from battalion commander to company commander, but rarely up from company to battalion or to adjacent companies. Every company had a radio operator that relayed and translated information between company and the TOC, which helped overcome language barriers, but caused a lag in message delivery, receipt and return. Furthermore, this meant companies did not operate on a battalion radio network. Information flowed separately to the TOC from company radio networks rather than across a battalion network. Each company liaison relayed messages to the TOC battle captain, who had no means of communicating directly with a company commander.

The best practice observed for C2 interoperability in multinational units is the employment of a liaison officer. Liaison officers can serve as a bridge to overcome constraints on digital system interoperability. If units focus their efforts on training and emplacing a liaison it could potentially mean the difference between mission success and failure. What digital systems lack in flexibility, a



competent liaison officer or team can achieve.

The NATO Handbook for Coalition Operations, indicates “the value of training assistance and dedicated liaison teams cannot be overstated, particularly when working between a force with digital warfighting capability and a force that works with analog means” (NATO Standard APP-13 Coalition Operations Handbook, Edition A, Version 1, section 7-5, November 2013). In employing liaison teams, many factors need to be considered in order for that team to be effective. Not only should they be deployed with a robust equipment list, enabling them with all the capabilities and assets necessary to maintain redundant communications with their parent unit, but also be properly trained on those systems such as Command Post of the Future, Blue Force Tracker and tactical satellite radio systems. It is falsely assumed that if digital systems are provided for liaisons interoperability will be achieved; on the contrary, those digital systems are often underutilized or not used at all.

In addition to training liaisons to use the equipment they are outfitted with, training them on their roles and responsibilities helps ensure they achieve the desired effects. “Liaison can reduce interoperability friction through direct communications, and contributes towards unity of effort, force integrity, and mutual support between different components of the force. It is used in all phases of operations, as well as during routine activity between units, to help facilitate, preserve freedom of action and maintain flexibility” (NATO ATP-3.2.2 Command and Control of Allied Forces, Annex G, section

G102, Feb 2009). Liaisons, in dealing with multinational operations, should be selected based off confidence, sensitivity, and awareness. A liaison officer who is tactful in the cultural differences of the NATO nation he or she is supporting, capable of navigating allied doctrine and, if possible, possesses language skills is trained and prepared to fully support multinational operations. Some liaisons may be empowered to represent the commander, and as such “chosen individuals should know their commanders, understand their commander’s plans and be able to cognitively express their commander’s views and intent to the command and HQ staff to which they are attached” (NATO ATP-3.2.2 Command and Control of Allied Forces, Annex G, section 105a, Feb 2009). It is the easy and flawed solution to assume that digital systems can contribute to interoperability to the same degree as well-trained and well-equipped liaison teams. Even in the absence of certain communication capabilities, the right liaison has the potential to overcome any gaps in interoperability.

Interoperability is necessary for maintaining effective command and control of a multinational unit and establishing operational

advantage. Digital systems seem to be the easiest solution, but rarely do digital systems achieve interoperability to a level that is effective. Establishing a common operating picture is crucial, and while digital systems can contribute to positive C2 for the commander, when numerous allied nations are involved digital systems present many constraints that are challenging to overcome. Many factors prohibit digital systems from cross-talking smoothly across any platform and with any NATO nation, and emphasizing the importance of training and emplacing a liaison is a great way to bridge any digital C2 gaps. By incorporating all aspects of C2 systems: personnel; doctrine; standard operating procedures and digital systems, interoperability can be enhanced to best support mission success. All methods must be exhausted to their fullest, with special emphasis and attention placed on liaison teams and their development.

CPT Brittany Coughran is currently assigned as an observer/controller-trainer of mechanized/maneuver and multinational units at the Joint Multinational Readiness Center in Hohenfels, Germany. She was commissioned as a second lieutenant in the Signal Corps in 2008 from the U. S. Military Academy.

ACRONYM QuickScan

BFT - Blue Force Tracker
C2 - Command and Control
COMSEC - Communications Security
CONET - Coalition Network
CPOF - Command Post of the Future
JMRC - Joint Multinational Readiness Center
MIP - Multilateral Interoperability Program
OC/T - Observer-Controller/Trainer
TOC - Tactical Operations Center

Mission Command Systems Integration in a Decisive Action Training Environment

CPT Julie A. Leggett

The decisive action training environment is an ideal scenario to implement a task-force structure. A task force with a hybrid organization provides a more robust capability set and enables flexibility within the large and fluid battlefield that is the DATE setting. While tactically ideal, however, the task force assembly imposes serious integration challenges for successful combined arms maneuver. The merge of different units with varying capabilities requires extensive effort to integrate mission command systems for decisive action.

The Challenge

Recently, the 3rd Armored Brigade Combat Team, 1st Cavalry Division deployed to the National Training Center with a hybrid task organization. With only one of three organic combined arms battalions available for the rotation, the Brigade Taskforce was comprised of a variety of augmentees. The attached units included 4-17 Infantry (Stryker) from 1st Brigade, 1st Armored Division; 3-66 Armor from 1st Brigade, 1st Infantry Division; a Long-range Reconnaissance and Surveillance Detachment from 504th Battlefield Surveillance Brigade, III Corps; and 395th Combat Sustainment Support Battalion from the Connecticut National Guard. A major challenge in managing such

a diverse organization was to ensure that each unit's unique and differing mission command systems were compatible. Most notable of these system differences were the unit's Warfighter Information Network-Tactical systems and Blue Force Tracker /Force XXI Battle Command Brigade and Below.

The WIN-T systems were a unique problem set. With the organic Brigade elements and other attached units operating WIN-T Increment 1b, 4-17 Infantry was utilizing the newly-fielded WIN-T Increment 2. WIN-T Increment 2 is drastically different than 1b, providing on-the-move capability and network extension down to company level. While WIN-T INC 1b and INC 2 are totally interoperable, however, there are major considerations when planning a dual-increment network. Primarily, consider the satellite band on which both units operate. Most units will have their systems pre-configured to operate on either Ku (a commercial satellite band) or Ka (government-only satellites), as all versions of WIN-T are equipped with kits to operate on either band. While WIN-T Increment 1 units are generally still utilizing Ku for CONUS operations, WIN-T Increment 2 units will almost always utilize the Ka satellite band due to funding (to purchase commercial satellite time for a bandwidth-heavy Increment 2 unit would be a considerably higher cost for the DOD). To operate fully

integrated network with limited latency, the task force must plan to utilize the same satellite band. If not, the latency would be twice as great due to the two-hops the transmission will take to traverse over both satellites bands. For this reason, units should plan to operate Ka band during all operations involving Increment 2 units.

The second major challenge in mission command systems integration was joining the FFCB2 and BFT networks. While Joint Capabilities Release software is interoperable with all versions of BFT, 3/1 ABCT organic Brigade elements operated FFCB2 (with Enhanced Position Location Reporting System radio terrestrial backbone) and software version 6.5, which was not automatically interoperable with BFT. In order to generate shared position location information (otherwise known as "blue dot") feed between organic brigade FFCB2 platforms, attached unit BFT platforms, and other Army Battle Command Systems, the unit had to complete three steps. First, submit all unit role names for the operation to Project Manager Joint Battle Command - Platform at least 30 days prior to the operation. Submitting URNs in a trouble-ticket through the Mission Command Support Center (formerly BFT Global Network Operations Center) website (<https://fcb2-bfthelp.army.mil/fsc/>) allows the administrators at PM JBC-P to connect the unit databases and network



advertisement across all the platforms on their end. Next, the unit must request and configure a Generic Routing Encapsulation tunnel for the Brigade command posts. The GRE tunnel is pointed to routers at the command posts to connect the unit's EPLRS backbone to the MCSC and allow the shared PLI feed of the combined database to publish down into the unit network.

Lastly, the unit must install and operate their FBCB2 ABCS Interoperability Client. The AIC connects to the unit's servers to publish and subscribe PLI feed between ABCS systems. This is the final step of the process which publishes the shared PLI feed into the Publish and Subscribe Server, making it accessible by the unit's battle staff that operates the Command Post of the Future and other ABCS systems.

"A Way"

Successful mission command systems integration is obviously not something that will happen by chance. It is not born from the fervent prayers of an S6, helpful over-the-shoulder guidance of an observer controller, or the magical actions of field service

representatives. It is a highly technical operation that requires deliberate planning and action across all units and elements involved. To achieve success, commanders and signal officers at all levels must prioritize early planning and synchronization.

If possible, start planning integration solutions at least three months in advance of the operation. Include the attached units in Technical Integration Working Groups to ensure all hardware and software will be fully compatible and that there are no ip-space conflicts and provide direct liaison authorization for sections and units in the task force to coordinate and report. These steps are a necessary part of integration planning, which will synchronize efforts and ultimately help to build the team.

In addition to early planning, the task force should conduct at least one combined command post exercise to test the network prior to the deployment or operation. Network testing will allow the units to make necessary reconfigurations and arrive ready to conduct an information assurance validation without having to troubleshoot

integration challenges on the spot. Additionally, a joint exercise will allow the Brigade to assess the training capabilities and deficits of all units, including those attached, to help cover any shortfalls prior to the deployment or operation. Lastly, since early network testing will result in an earlier and easier completion of an IA validation, it will consequently provide more time to complete a full mission command rehearsal exercise prior to deployment, which is also essential for success in a DATE setting.

A final source for integration success is to maximize use of all available systems. This will help to provide redundancy and flexibility across the spectrum of varying units and capabilities. Particularly, there are two major signal capabilities organic to a BCT that are often underutilized. The first is the high-capacity line-of-sight system. Even when limited to 2mB of bandwidth (as is the case at the NTC), users notice drastic improvement in network speed, virtually eliminating lag for phone calls and latency with SharePoint and other services. When HCLOS

(Continued on page 56)

(Continued from page 55)

(v)1's are properly distributed (think the four most rearward battalions: Brigade Support, Aviation, Engineers, and Field Artillery), the HCLOS network can be a tremendous asset for the task force throughout every stage of the battle.

The other underutilized asset is the Tactical Operations Center Intercommunications System. Most 25-series know that a properly configured TOCNET provides a true Integrated Tactical Network Environment, with capabilities to transmit voice communications interchangeably between what is formerly referred to as upper tactical internet and lower tactical internet. The aspect that some units fail to utilize, however, is implementing TOCNET to almost eliminate the need for Brigade-level radio retransmission operations. This is possible because you can have subordinate command posts log into the Brigade Main's Micro Central Switching Unit from their remote locations via the Soft Crew Access Unit. Utilizing

Soft CAU at the distant ends allows the radio signals to travel over the upper TI (satellite infrastructure) for a limitless distance, eliminating traditional line-of-site requirements for radio communications between command posts. The only residual need for RETRANS, then, is during initial command post establishment and while commanders and leaders are communicating from mounted platforms.

Conclusion

The DATE provides one of the most profound training experiences our Army offers, and not just for the maneuver aspect. Providing a reliable communications backbone in a DATE scenario is one of the greatest challenges for modern signaleers. When a task force with varying capabilities is combined for a decisive action fight, the problem set is exponentially increased. Deliberate planning, testing, and training are necessary to achieve mission command integration. To accomplish success, Signaleers should plan

integration months in advance and utilize all available systems to their full extent. Signal as much as any warfighting function relies very much on the "train as you fight" mindset, and in order to fight a task force in a decisive action environment, signaleers must conduct testing prior to the rotation. It would be a grave mistake to just show up to a DATE with a newly joined taskforce and assume since all systems are technically interoperable they will easily integrate.

CPT Julie A. Leggett currently serves as the Brigade S6 for 3rd Armored Brigade Combat Team, 1st Cavalry Division at Fort Hood, TX. She commanded the Signal Company in the same brigade. She is from Sunman, Ind. and has a Bachelor's degree in Political Science from Wheaton College and a Master's Degree in Information Technology Management from Webster University.

Join the Discussion

<https://SIGKN.army.mil>



ACRONYM QuickScan

ABCS – Army Battle Command System
ABCT – Armored Brigade Combat Team
AIC – ABCS Interoperability Client
BFT – Blue Force Tracker
BGN – BFT Global Network Operations Center
CAU – Crew Access Unit
CPOF – Command Post of the Future
DATE – Decisive Action Training Environment
DIRLAUTH – Direct Liaison Authorization
EPLRS – Enhanced Position Location Reporting System
FSR – Field Service Representative
GRE – Generic Routing Encapsulation
HCLOS – High-Capacity Line-of-Sight
IA – Information Assurance

ITNE – Integrated Tactical Network Environment
JCR – Joint Capabilities Release
MCSC – Mission Command Support Center
NTC – National Training Center
PASS – Publish and Subscribe Server
PLI – Position Location Information
PM JBC-P – Project Manager Joint Battle Command-Platform
RETRANS – Retransmission
TIWG – Technical Integration Working Group
TOCNET – Tactical Operations Center Intercommunications System
TI – Tactical Internet
URN – Unit Role Name
WIN-T – Warfighter Information Network-Tactical

Submit an article to The Army Communicator

The Army Communicator is the U.S. Army Signal Regiment's professional journal, exploring trends in the Regiment and providing a place for Signal Regiment members to share accomplishments, ideas and lessons-learned with their colleagues.

The Army Communicator depends on non-commissioned officers, officers, warrant officers and Regimental civilian employees to contribute quality articles on topics of interest to the entire Regiment.

We invite all our readers to submit articles, write letters to the editor or contact us if you have any questions, comments or suggestions.

How to submit an article

Steps involved in submitting an article to AC are outlined following: Select a relevant topic of interest to the U.S. Army Signal Regiment / military information-technology community. The topic must professionally develop members of the U.S. Army Signal Regiment.

Write an outline to organize your work. Put the bottom line up front and write clear, concise introduction and conclusion paragraphs.

Follow the writing standard established in AR 25-50, Preparing and Managing Correspondence, Section IV (the Army writing style), and DA Pamphlet 600-67, Effective Writing for Army Leaders, especially Paragraphs 3-1 and 3-2. The Army standard is writing you can understand in a single rapid reading and is generally free of errors in grammar, mechanics and usage. Write as if you were telling someone face-to-face about your subject.

Send the article to the editor Larry Edmond at Larry.e.edmond.civ.@mail.mil Or place a copy of the article on AKO in the "Articles for Submission" folder and send a notification email to the Army Communicator editor.



OFFICIAL BUSINESS
ISSN 0362-5745



On March 11, 2016, a Signal Ball was held in Reston, Va. During the event, 11 very deserving people were inducted as Distinguished Members of the Signal Regiment. LTG Robert S. Ferrell, CIO/G6 (fifth from left), is shown above with 10 of the inductees or their representatives. The next edition of the Army Communicator will feature their stories.

Since the activation of the Regimental system, we have had a program for recognizing people who have made a special contribution or who have distinguished themselves in service to the Regiment.

Distinguished Members of the Regiment are prestigious or notable military or civilian persons who are recognized for their accomplishments. The designation as a Distinguished Member of the Regiment serves to perpetuate the history and traditions of the Regiment, thereby enhancing unit morale and esprit de corps.

