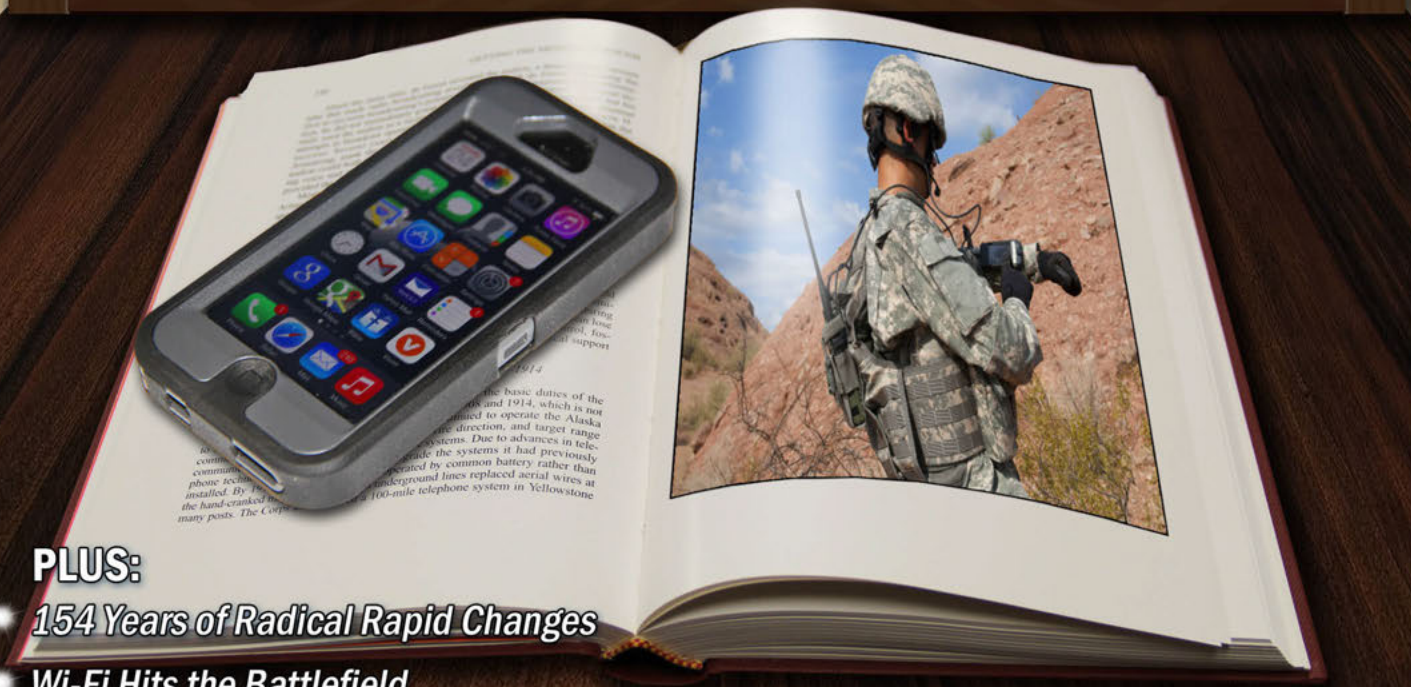
Approved for public release;
distribution is unlimited.
Headquarters,
Department of the Army

ARMY COMMUNICATOR

Voice of the Signal Regiment

PB 11-14-2 2014 Vol. 39 No. 2

SIGNAL TRANSFORMATIONS



PLUS:

- *154 Years of Radical Rapid Changes*
- *Wi-Fi Hits the Battlefield*
- *Cyberspace Lessons Learned*
- *New spectrum sharing approaches*

Chief of Signal

MG LaWarren V. Patterson

Cyberspace operations offers new opportunities

Greetings Signaleers,

As the Army transitions to a more cyber-centric future, it is easy to lose sight of the role the Signal Corps has played—and will continue to play—in shaping that future. But the truth is that the Signal Corps plays not just a critical role in Cyberspace Operations, but also possesses the keys of innovation that will enable the rest of our Army to achieve its strategic goals.

"Our role both in Cyberspace Operations and in developing the future of the Army shows us that the Signal Regiment is more relevant than ever.

In my 32 years of service, I have seen the Signal Corps change. As you'll read in this issue, we've undergone several major realignments since our inception 154 years ago. As the first to take interest in the capabilities of the airplane, we spawned the Army Air Corps, which evolved its own service—the U.S. Air Force. We created the National Weather Service, which now reports to the Commerce Department, under the National Oceanic and Atmospheric Administration. More recently, in the early 1990s, the Signal Regiment lost over 400 of its best and brightest to help stand up the newly-created Army Acquisition Corps.

It would be false to claim that the Regiment did not experience some pain after each of those aforementioned changes. And yet we not only survived, but we grew stronger. In fact, the Signal Corps is stronger now than it was during any of those transitional periods. Our mission is more important than ever. Our modern tools possess unprecedented capabilities previously relegated to science-fiction. And our Signaleers are of the highest educational caliber the nation has yet seen.

One significant Army strategic goal is outlined in "Force 2025 and Beyond." Intended to prevent future technological overmatch, Force 2025 and Beyond explores how to redesign the Army to match presently unforeseen challenges and ultimately field a tactically-agile Army that possesses greater efficiency and lethality. Crucial to this effort is the development of key technologies that will enable our Signal Corps to provide a network that meets the communication needs of this future Army. We must explore exciting issues such as the challenge of operating in a GPS-denied environment, increased modularity through hardware/software convergence, and the implementation of data fusion to achieve cyber situational awareness. The key to our success will continue to be found in the adaptive leaders—officer, warrant, and NCO—that we possess in our Regiment.

In the days ahead, even as the Chief of Signal position mantle is transferred from the Cyber Center of Excellence level to the Signal Commandant, the Signal Corps will maintain its commitment to technical and tactical excellence. We will continue providing our Army with the tactical and strategic communications it needs to achieve its goals now and in the future. Our role both in Cyberspace Operations and in developing the future of the Army shows us that the Signal Regiment is more relevant than ever. We give our Army 'The voice to give command' and we will continue to do so!

Pro Patria Vigilans—Watchful, for the Country!

Join the Discussion

https://SIGKN.army.mil

U.S. Army Cyber Center of Excellence
fort gordon

Command

Chief of Signal
MG LaWarren V. Patterson

Regimental Chief Warrant Officer
CW5 Peter T. Winter

Regimental Command Sergeant Major
CSM Ronald S. Pflieger

Editorial Staff

Editor-in-Chief
Larry Edmond

Art Director/Graphic Designer
Billy Cheney

Photography
Billy Cheney, Amy Walker, Richard Bumgardner, SGT Javier Amador, Bruce Brim

By Order of the Secretary of the Army
Raymond T. Odierno
General, United States Army
Chief of Staff

Official:

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

Authorization 1418906

Army Communicator (ISSN 0362-5745) (USPS 305-470) is published quarterly by the U.S. Army Cyber Center, of Excellence 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 Cyber Center of Excellence, 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 Cyber Center of Excellence, 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 Cyber Center of Excellence and Fort Gordon, 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.***

Worldwide web homepage address
http://www.signal.Army.mil/ocos/AC/
E-mail: ACeditor@conus.Army.mil

PB 11-14-02
Summer 2014
Vol. 39 No. 2

Army Communicator

Voice of the Signal Regiment

Table of Contents

Features

5 **The Enduring Signal Corps Pioneering Innovations**
Steven J. Rauch

16 **Wi-Fi Hits the Battlefield**
Amy Walker

19 **Command and General Staff College Transforming Signal Education**
Michael H. McMurphy
Gregory Thomas

21 **Master Gunner Training Keeping Pace with Latest Technology**
Nancy Jones-Bonbrest

24 **Soldier Input Fuels Network Hotspot Evolution**
Claire Heininger

26 **LandWarNet Primer**
Patrick S. Baker

28 **Adapting the Network to the Mission**
MAJ Graham Wood

33 **Collaborative Spectrum Management**
SFC Nicholas A. Perez-Santalla

38 **Sharing the Electromagnetic Spectrum**
CPT Bryant A. Wellman
CW5 Garth R. Hahn

44 **Starnet Roadmap for the Future Network**
Claire Heininger

48 **New Satellite Terminal Program Increases Capacity**
Amy Walker

51 **Enterprise Security System Deployment**
MAJ Scott A. Salmon

53 **Operating an Effective Afghanistan Network**
COL Stephen Hager

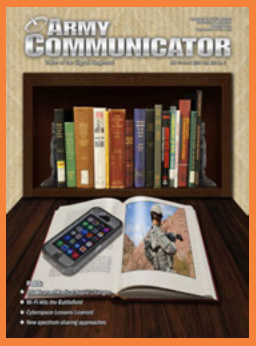
56 **Signal Retrograde from Afghanistan**
COL Linda C. Jantzen
LTC Jeffrey J. Thompson

61 **Main Communications Facility Start-up**
LTC Pam Boyle
MAJ Jacob Cox

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

Get connected with the latest on cyberspace lessons learned in a Mission Command Center of Excellence bulletin. See details on ***Page 65****.*

Cover: *As the Signal Corps realigns to meet the ubiquitous mission requirements of cyperspace operations, this edition looks back at some of the other major shifts the Regiment has negotiated in our 154 years. The result is the Signal Corps always emerges stronger with our core mission in tact and relevant as ever.*



Cover design by Billy Cheney

Signal Regiment embracing changes

Signaleers,

Prior to assuming my position as deputy to the commanding general, I spent over four years running the Software Engineering Center at the Communications Electronics Command. We supported all the CECOM and associated PEO systems with software. The majority of those systems belonged to the Signal Corps. My experiences served as a learning introduction to Army software tools, and I had the opportunity to interact with various systems such as WIN-T, JWICS, ABCS, CNR, DCGS-A, CPOF, SINGARS, and others. When I became the SEC director we had a budget of $800 million which grew to a staggering $1.4 billion during my four plus years of leadership.

Two of our greatest areas of growth were in system support for the DCGS-A component, and the implementation of a field support directorate with over 700 Field Service Representatives and Field Software Engineers. While I received many accolades from my customers on the level of service provided through these representatives, many commanders lamented the inability of their own formations to perform set up maintenance work on these vital signal systems. It seems like destiny that my next assignment would be with the command team at the then Signal Center of Excellence.

While I had a solid grasp on Signal systems, I did not yet know the Signal Regiment as well as I would have liked. Rightfully so, in the year that has followed, I have been continuously impressed by the breadth and depth of talent and knowledge I have encountered throughout all echelons of the Signal Regiment—officer, warrant officer and enlisted.

While still proud of the level of support my staff at CECOM was able to provide to the Army, I am now equally thrilled that the Signal Regiment is again embracing its role as both operator and maintainer of its equipment. For me, the primary reason for the Signal Corps' existence is that, when going to war, we begin by destroying the enemy's command and control infrastructure. Then our Signal Corps rebuilds the communications infrastructure for our network-dependent Army. The Signal Corps is a vital element of our Army today and will continue to be even more so in the future. Once established, the operation and maintenance of the network begins. Cyber space domination is a critical element in the equation required for operating and maintaining the networks. Cyberspace operations expand our responsibility for building and maintaining functional, reliable and secure networks.

The Signal Regiment has been and always will be necessary. There is no need to fear the emergence of cyber. As builders, operators and maintainers of the LandWarNet, the Signal Corps supports the Army portion of the DoD Information Network—which, together with offensive and defensive cyberspace operations, form the three components of Cyberspace Operations. As members of the Signal Regiment expand our ability to self-sustain, we will increasingly find ourselves even more vital to the conduct of military operations by giving our Army the needed network agility and security both on land and in cyberspace.

Signal Corps critical to Army success

Signaleers,

Members of the Army Signal Corps are more relevant today than ever. And more important the Regiment will continue growing as demand increases to build, maintain, operate, defend and secure the warfighter network.

Today's expeditionary land forces demand mobility and rapid network connectivity to send and receive tactically-relevant information. Warfighters require a single end-to-end network that fully supports and enables mission command with little to no deployment notice.

In the years ahead, we must grow our internal capabilities, learn to leverage commercial networks, and explore ways to better disseminate intelligence to the lowest level all while staying on the cutting edge of technology and training. Now, let me unpack these three fascinating topics.

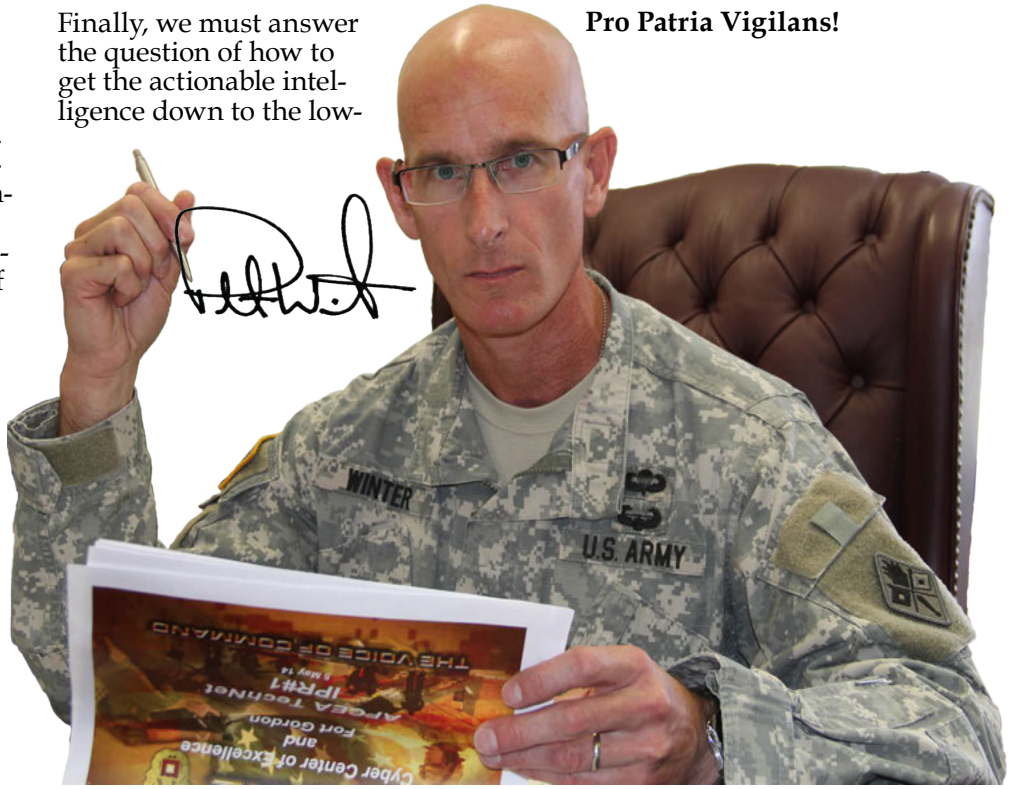
Tactical and technical proficiency remains as important as ever in providing information superiority. Warfighter Information Network – Tactical systems is the Army's communications program delivering state-of the-art commercial-off-the-shelf and government-off-the-shelf communications capabilities. As new capabilities are rolled out we must ensure we can fully utilize and are familiar with the technology fielded to our units. Stay plugged into the school and look for and demand live, virtual, constructive integrated training. As budget cuts result in a more streamlined field service representatives support force, our own Signaleers must pick up the torch, developing expert troubleshooting and maintenance skill sets. The end result will be a Signal force that is increasingly self-sustaining and self-repairing.

Another area for growth is the exploration of integrated networks. Whether leveraging organic host nation networks, or even tapping into our own commercial assets, we must continue the press to provide robust communications and capabilities at all phases of military operations. Army forces must be networked, linked and synchronized in time and purpose to enable more efficiency as dispersed forces attempt to communicate, maneuver, share information, collaborate and develop a common operating picture. Of course, we will need to work closely with our cyber peers to mitigate security risks found in the less-secure networks that we will undoubtedly encounter. But by anticipating these challenges, we can create network architectures that will provide confidentiality, integrity, availability and security while enabling us to draw on existing network infrastructure.

Finally, we must answer the question of how to get the actionable intelligence down to the lowest level. We cannot fully exploit the staggering quantities of intelligence we collect unless we can transmit it promptly and accurately to those on the front lines who require it. The special operations community has led the way in disseminating last-minute intelligence updates. Developing the methods and technology to field that same capability to the rest of the Army will be a combat force-multiplier.

Critical to achieving any of these goals are our functional area and warrant officer experts. With an eye on the strategic picture, Signal Corps leaders and planners are relying on each member of the Regiment to think outside the box, developing tactically sound but operationally creative solutions that will enable our Army to leverage and integrate emerging technologies. The Signal Corps is the Army's information technology provider and remains integral to the Army's success.

Pro Patria Vigilans!



Moving on

Future bright for the Signal Regiment

Signaleers,

As I sit at this seminal point preparing to retire and crafting this last message to you as a Soldier and regimental command sergeant major, I find myself experiencing a unique perspective from which to view my service, the Signal Regiment and the Army.

While some critically important elements remain the same, much has changed since I entered the force over three decades ago.

My first assignment was as a radio operator with A Company, 16th Signal Battalion, 3rd Signal Brigade, based out of Fort Hood, Texas. My unit was assigned AN/GRC-50 radios—the "Angry 50." They were heavy, awkward and slow multi-channel radios—quite different from the AN/GRC-245 used by high capacity line of sight operators today! But today's 25Q Signaleers who operate our modern multi-channel radios share the same mission—providing tactical communications to the troops on the ground.

The same can be said for each unique position I held. As the 82nd Airborne Division's battlefield spectrum manager, I worked with tools that were the predecessors of today's "Spectrum XXI," used by 25E electromagnetic spectrum managers. As the J6 operations sergeant in Korea, I interfaced with the strategic side of Signal, and as command sergeant major of the Joint Communication Support Element (Airborne), I employed the kind of cutting-edge equipment only found in the special operations community.

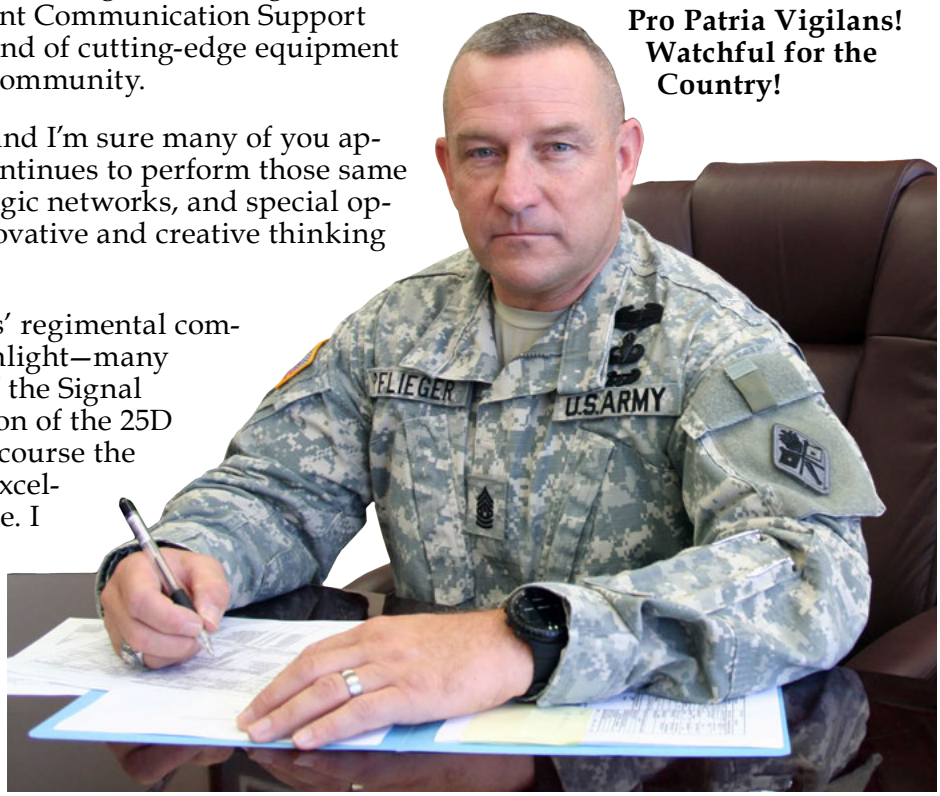
The tools of the trade have changed, and I'm sure many of you appreciate that! But the Signal Corps continues to perform those same jobs—tactical radio, tactical and strategic networks, and special operations support— with the same innovative and creative thinking that I remember.

During my tenure as the Signal Corps' regimental command sergeant major—my career highlight—many changies occurred: transformation of the Signal Corps' enlisted MOS structure, creation of the 25D cyber network defender MOS, and of course the transition from the Signal Center of Excellence to the Cyber Center of Excellence. I can confidently say that, working closely with our cyber partners, the Signal Corps of the future will soon possess capabilities far beyond what I ever imagined when I enlisted in 1982.

So as I look back over my 32-year career, I see the many ways in which the Army and the Signal Corps have changed. But I also see a Signal Corps that has continued to excel at its core mission: providing leaders and Soldiers the ability to communicate. Throughout all the changes, the Signal Corps members have remained resilient and always at the cutting edge of technology.

It has been my privilege to serve with each and every one of you! As I prepare to move on, I will keep my ear to the ground and look forward to hearing about the future accomplishments of the Signal Corps.

Pro Patria Vigilans!
Watchful for the Country!



The Enduring Signal Corps

Pioneering innovations since 1860

By Steven J. Rauch

In March 2014, the U.S. Army Signal Center of Excellence was re-designated the U.S. Army Cyber Center of Excellence and tasked to lead efforts for developing experts to dominate cyberspace operations.

As members of the U.S. Army Signal Corps adapt to this pioneering role, it is worth taking a moment to look back in history and examine similar significant milestones that radically changed the course but not the core mission of the branch.

Enabling communications is the core mission of the Signal Corps because communications are an essential element for achieving success in military operations. Commanders must have effective communications to maintain command and control over their forces without regard to physical distance, whether it is on land, on the sea, in the air, in space, or today – throughout cyberspace.

The article intends to illustrate that when called upon to explore new technologies or pioneer unique missions no other branch was capable of executing, the U.S. Army Signal Corps often assumed significant organizational risk that jeopardized existing force structure or its identity, but it did not vanish and it will not disappear during the assumption of this new mission. The Signal Regiment will continue. The Signal School will still exist as a subordinate entity of the Cyber Center of Excellence. The U.S. Army Signal School will continue producing trained Signal Soldiers to provide reliable, rapid and global communications for the Army. Fort Gordon, Ga., will still be home to the Chief of Signal and the U.S. Army Signal Corps regiment where the history and heritage of over 154 years of service will continue to contribute to both established and emerging domains of warfare.

BG Albert J. Myer, inventor of the wig-wag communications system, founder of the Signal Corps and chief signal officer until his death in 1880.

Land Domain

The U.S. Army Signal Corps, established by Congress on 21 June 1860, became the first military organization in any nation solely dedicated to installing, maintaining and operating tactical land communications.

The creation of the Signal Corps coincided with technological advances that expanded the size of traditional battlefields, requiring new methods of communication beyond voice commands and couriers.

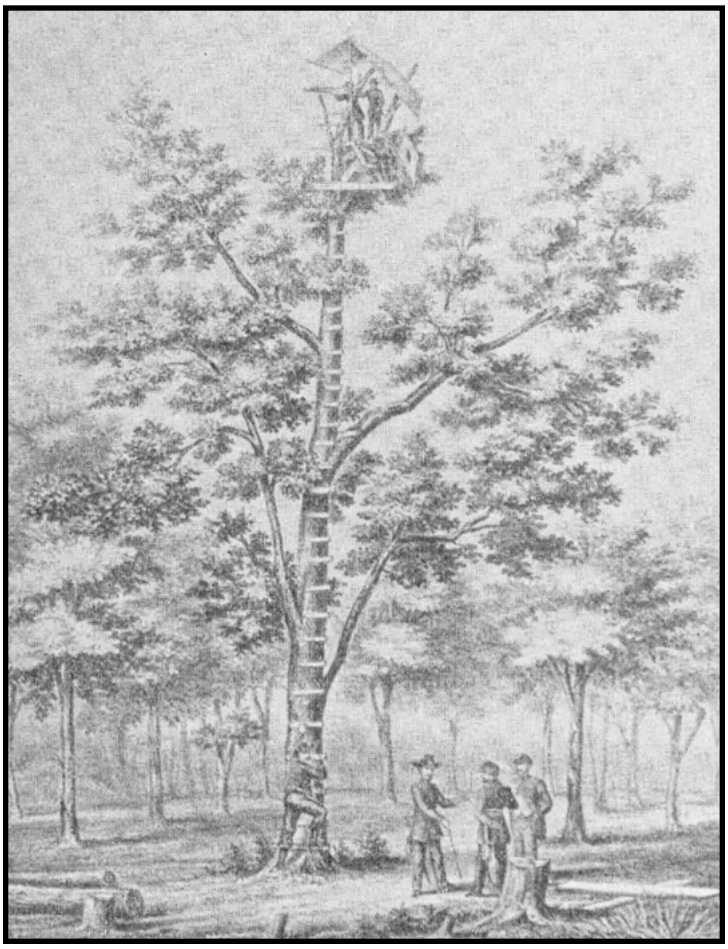
An Army doctor, Albert J. Myer, had devised a visual communications system known as Wig-Wag, which used a flag by day or a torch at night to rapidly send messages over long distances. Only one flag or torch was used at a time and field telescopes were employed to read the messages between signal stations. The operators of the wig-wag could typically send three words a minute over an average distance of ten miles between stations.

(Continued on page 6)

(Continued from page 5)

Upon acceptance of his communications system by the Army, Myer was appointed to the rank of major and chief signal officer to organize a corps of Soldiers trained in tactical signaling. During the U.S. Civil War, signal Soldiers deployed in tree tops, on roof tops, and on signal towers to send and receive important messages for their supported commanders. Signaleers were dispatched on reconnaissance missions and attempted to read enemy wig-wag flag messages as well. This led to the development of various encryption methods to provide information assurance and safeguard the secrecy of orders during operations.

Often the wig-wag tactical networks changed the outcome of a battle, such as Gettysburg in July 1863. During the battle, the Signal Corps provided timely information to enable Union commanders to seize several tactical and geographic opportunities before the Confederate army could react. CPT Lemuel Norton served as the Army of the Potomac chief signal officer (a G6 today) and worked closely with the commander, MG George G. Meade, throughout the battle. Signal teams were positioned in order to provide a fully integrated wig-wag tactical network to support Union defensive operations.



Example of installation, operation and maintenance of the wig-wag tactical system during the Atlanta Campaign in 1864.

One critical wig-wag station was on Little Round Top at the extreme left of the Union line where signaleers could observe and report the enemy's tactical movements. The presence of this wig-wag station effectively hindered and provided early warning of the attempt by LTG James Longstreet's men to outflank the Union left on 2 July 1863. Ironically, LTG Longstreet's chief of artillery was LTC Edward P. Alexander, who had once served as MAJ Myer's assistant and was fully aware of the capabilities of the Signal Corps. LTC Alexander would later claim "that wretched little signal station" as the reason the attack failed at Little Round Top.

Unfortunately, it would not be until long after the Civil War when the Signal Corps contribution to land operations would be recognized for its significance. Though there were many episodes of individual signal Soldiers performing great feats of wig-wagging, code breaking, and even intelligence gathering, the infant Signal Corps was seen by most senior Army leaders as an interesting, but non-essential organization. As long as the Signal Corps did not require significant fiscal or manpower resources, then its existence was tolerable. This reality did not bode well for MAJ Myer's offspring in the post-Civil War period when the War Department reduced its force structure from over one million Soldiers in 1865 to 57,000 in 1867, 38,000 by 1870, and its lowest point of less than 25,000 active Soldiers in the entire U.S. Army in 1877. In that scarce fiscal and manpower environment, many Army leaders believed there was no room for a luxury like the Signal Corps.

SEA DOMAIN

During the course of the Civil War, the U.S. Navy had conducted numerous joint operations with the Army along the coasts and major rivers to provide transportation of troops and supplies as well as ship to shore fires capability. To facilitate command and control, Signal Corps personnel were embedded upon U.S. Navy ships so that ground commanders could quickly transmit requests for supplies, transport or fires through the wig-wag system.

In fall 1864, MG William T. Sherman began a march through Georgia with over 60,000 men to the seaport of Savannah. As the Army closed on its objective in mid-December, MG Sherman sought to establish contact with the U.S. Navy ships that were carrying much needed supplies, medical support and artillery capability. One remaining obstacle to be overcome was Fort McAllister, a small confederate outpost located on the Ogeechee River that needed to be seized so that ships could safely navigate the river and link up with MG Sherman's army.

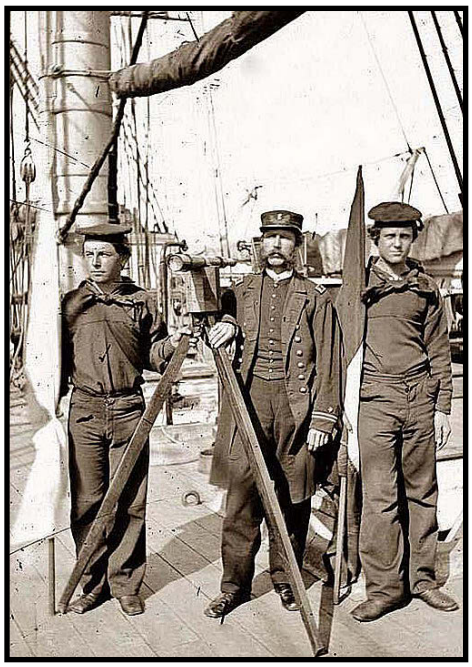
The embedded signal teams within the Union Army and Navy command structure enabled coordination for this mission. CPT James M. McClintock, chief signal officer, Army of the Tennessee, reported, "On the 11th [Dec] [we] established a station of observation at a rice mill on the Great Ogeechee two miles and a half north of Fort McAllister. A strict watch was kept [for] any vessel that might be near the mouth of the river."

Illustration by artist Don Troiani depicts the signal station at Cheves Rice Mill, December 1864 executing wig-wag communications with U.S. naval vessels in the Ogeechee River near Fort McAllister at the conclusion of Sherman's march to the sea.

BG William B. Hazen's division was selected to attack Fort McAllister on 13 December 1864 and his signal team established communications with McClintock at the rice mill to receive orders. During BG Hazen's attack, CPT McClintock's signal team spotted a navy ship in the river and immediately exchanged wig-wag messages with the Army signal team aboard the vessel. During a span of about 30 minutes, the signal teams had demonstrated how Myer's wig-wag system could provide combat commanders long range, line of sight, command and control to support both ground combat and naval communications.

After the Civil War, the success of this Army-Navy association inspired COL Myer to institutionalize and standardize signal training within the education systems of both services. In his annual report for 1867, COL Myer enthusiastically reported about a project to incorporate instruction of visual signaling and telegraphy at the U.S. Military Academy. The Army was behind in this training whereas the U.S. Navy had already committed to training cadets at Annapolis about Myer's wig-wag system. COL Myer hoped during future years to synchronize Signal equipment, doctrine and training between the Army and Navy to ensure interoperability

(Continued on page 8)



The U.S. Navy employed Myer's wig-wag system as illustrated by the flags and telescope to communicate with Army signal teams during coastal operations during the Civil War.

(Continued from page 7)

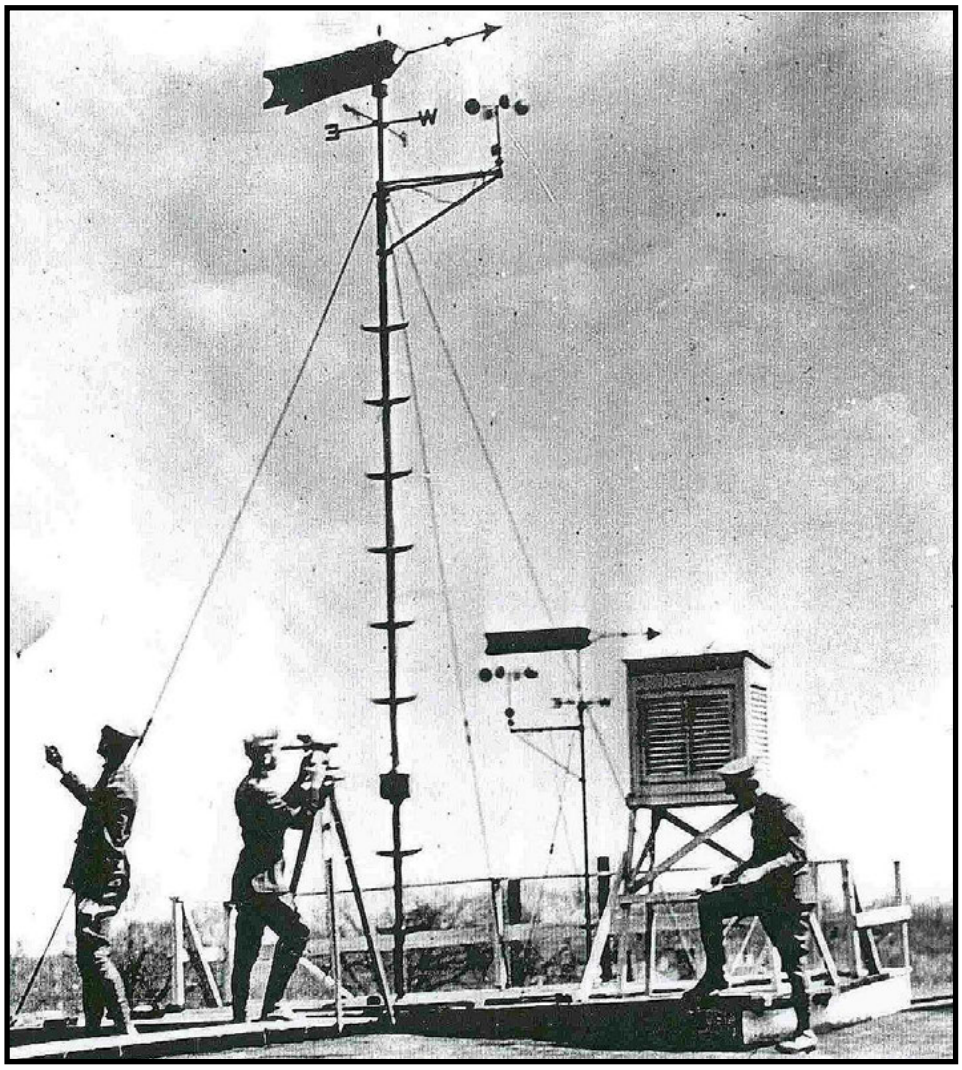
during future joint operations. COL Myer stated, "It will be cause for congratulation when the Naval and Military Academies of the United States have been the first to secure intelligent co-operation on which, in time of war, the fate of grand operations may depend." This quote illustrates how Myer was not only just an Army signal officer, but one of the first joint officers who sought to solve the issues of interoperability between forces operating simultaneously in both the land and sea domains of warfare.

COL Myer's vigorous promotion of joint communication had an effect on leaders in Congress and in 1869 they established the position of chief signal officer of the U.S. Navy. They also directed both Army and Navy chief signal officers to develop common signal training, message encryption, and any other methods to promote, improve and synchronize communications between the land and sea warfare domains.

This harmony was demonstrated in 1870 when the Navy Department adopted Myer's Manual of Signals, the signal doctrine for that time, and began sending navy and marine officers to attend the Fort Wipple (later Fort Myer) Signal Training School.

Information Domain

The drastic post-Civil War force reductions effectively reduced the U.S. Army to a skeletal force for the mission of policing the rapidly diminishing western frontier. Many Army leaders sought to protect their organizations and pet bureaucracies from cuts by finding new missions, many of which proved to be more civil than military in nature. One civil concern focused on meteorology and



Example of a U.S. Army Signal Corps operated weather station which gathered raw meteorological data which was then forwarded to Washington D.C. for analysis and publication as weather forecasts in local newspapers across the U.S.

how that science could be harnessed to improve information about weather conditions vital to an agricultural America. In 1869 these agricultural interests lobbied Congress to create a national organization to observe, report, and forecast the weather. Upon consideration, Congress determined these duties should be assigned to the U.S. Army because "military discipline would secure the greatest promptness, regularity and accuracy required in observations." Thus during a period of draconian force reductions, when Army leaders were questioning if they even needed a Signal Corps, then COL Albert J. Myer displayed a determination to save his creation. COL Myer took the initiative and contacted Congressional supporters who later said he had "a most intense desire that the execution of the law be entrusted to him."

On 15 March 1870, the secretary of war assigned the meteorological duties to the Signal Corps, undoubtedly saving it from passing into military history as a curious fad rather than an enduring organization.

From 1870 to 1891 the Signal Corps successfully operated the nation's first modern weather service using both commercial and military telegraph lines to report weather observations to Washington D.C. The observation stations were located after consultation with meteorologists based on previous courses of storms and availability of telegraph service in an area. Each Signal Corps meteorological station was manned by three Soldiers, led by a sergeant and equipped with a barometer, thermometer, hygrometer, anemometer, anemoscope (wind vane) and pluviometer (rain gauge).

After Soldiers collected the daily readings, they sent them via telegraph to the Signal Corps headquarters in Washington D.C., where the data was compiled and analyzed by civilian and military scientists to predict the weather for the next few days.

On a daily basis they produced an average of 35 weather bulletins and 60 weather maps which were then distributed to over 9,000 post offices and made available to local newspapers for publication. At least 1/3 of American households received Signal Corps produced weather information in some form, mainly through the newspapers. Thus by the time the newly promoted BG Myer died in 1880, the Signal Corps weather service was world renowned.

Unfortunately, that fame almost killed the Signal Corps when a new generation of civilian officials and military leaders began to question why the Army was funding and managing information that was essentially civilian in nature.

In 1884, a congressional committee concluded that, "the Signal Service is now a weather bureau with a corps of men performing this civil service while they are enlisted in the Army. The Army gets no benefit from this Signal Corps, and places no reliance upon it for military service."

A bill was introduced in Congress in 1890 that recommended the Signal Corps be abolished since it seemed to no longer have a military function. The bill was defeated, but another was offered that recommended the weather service be transferred to the Department of Agriculture.

The effective date for the transfer of the weather information mission was 1 July 1891 and after all of the equipment, stations and personnel were settled what remained of the U.S. Army Signal Corps was a hollow shell of an organization. The legislation also specified that Signal Corps missions would be restricted to "strictly military matters" and set the authorized strength at one brigadier general, one major, four captains, four first lieutenants, and 50 sergeants whose focus became the application of communication technology for the U.S. Army. It was from these seeds that a new Signal Corps would grow into the robust and enduring organization it would become shortly after the turn of the century.

One other aspect related to the information domain deserves mention during this period as it ties in to the topic of the information mission

(Continued on page 10)

(Continued from page 9)

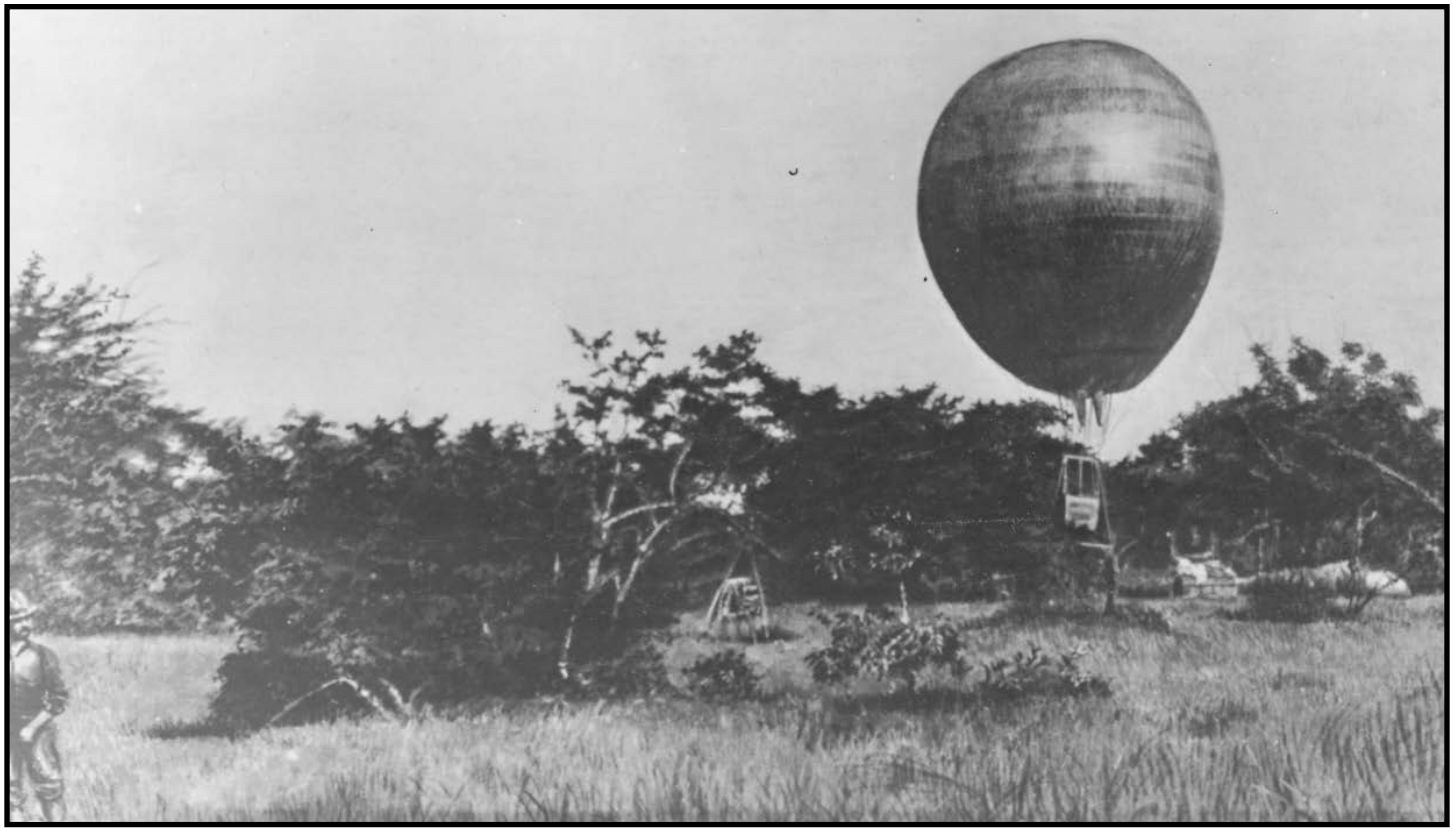
area that would occur almost 100 years later in the 1980s. In 1892, Chief Signal Officer BG Adolphus Greely sought to expand control over the military information function that belonged to the Adjutant General's Office. BG Greely claimed this mission was part of the Signal Corps task to "collect and transmit information for the Army" but he was unsuccessful in this endeavor. However in 1894 the Signal Corps did acquire supervisory responsibility for the War Department library, which included over 30,000 volumes and 6,000 glass-plate negatives of Civil War photographer Mathew Brady. Until 1904 when the Army divested the Signal Corps of this mission, the branch had doubled the number of volumes and introduced modern library techniques for information management.

Air Domain

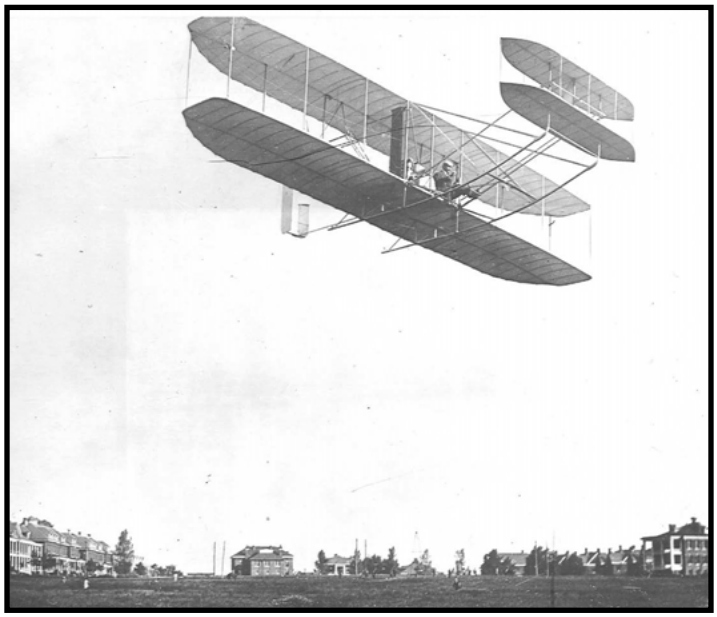
Since its beginning, the Signal Corps explored any technology that enabled clear line of sight for communications, to include aerial platforms such as balloons, dirigibles and later aircraft. As such, the Army recognized the Signal Corps as the branch with the skills and technical knowledge to pursue early military aeronautical technologies in the air domain of warfare.

In the late 1890s the Signal Corps explored the use of aerial communications, employing balloons as portable observation platforms. An anchor rope carried a telephone line from the basket to a ground station below manned by a team that could quickly relay the information obtained aloft to the appropriate ground commander. During the Spanish-American War, the Signal Corps applied this capability in Cuba to conduct reconnaissance for planning the attack on Spanish defenses at San Juan Hill. A Signal officer named LT Joseph Maxfield operated the balloon.

On 1 July 1898, LT Maxfield and LTC George F. Derby, an engineer observer, ascended near the enemy position at El Pozo. LTC Derby demanded that the ground crew move the balloon closer to the enemy positions. As the balloon



The Signal Corps balloon Albert J. Myer during operations in Cuba during the Spanish-American War in 1898 used to provide reconnaissance support to the infantry assault on San Juan and Kettle Hills.



Photograph of the 1908 flight trials conducted for the U.S. Army Signal Corps at Fort Myer, Va., as part of the development of aviation technology for military applications.

floated above the landscape, it gave the Spanish an excellent target. When the Spanish opened fire, shrapnel and bullets tore the balloon apart, but the two observers were not hurt. Luckily, the officers did observe a previously unknown trail in the woods that helped speed the deployment of U.S. infantry toward San Juan Hill.

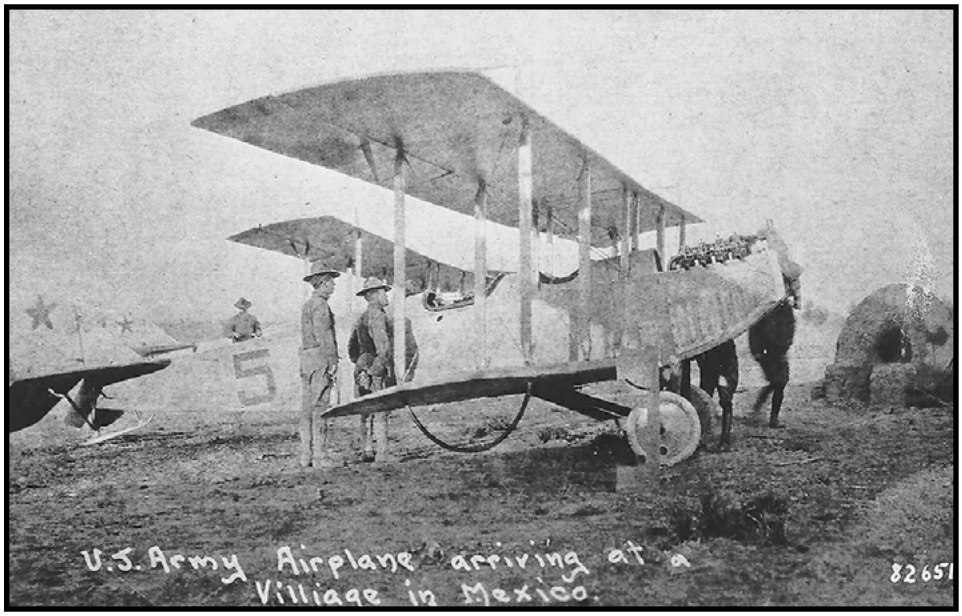
In 1906 Chief Signal Officer, BG James Allen placed considerable emphasis on aviation and his staff had been following the progress of two bicycle makers from Ohio, Wilbur and Orville Wright. The potential military application of the airplane clearly impressed Army leadership after the successful flight at Kitty Hawk, N.C., in December 1903.

On 1 August 1907, the Signal Corps established a small Aeronautical Division led by CPT Charles deForest Chandler to take "charge of all matters pertaining to military ballooning, air machines, and all kindred subjects."

On 23 December 1907, the Signal Corps issued a bid for an aircraft that could fly forty miles per hour and carry two people a distance of 125 miles. It had to stay airborne for at least an hour and land at the takeoff point undamaged. It also had to be easy to disassemble and transport. The Army received forty-one bids but only three met the specifications. Of those three, the Wright brothers were the only contractor to deliver an airplane. On 10 February 1908, the Wright brothers and the Signal Corps entered into a formal contract that provided for the delivery of an aircraft to Fort Myer, Va. Following several tests, evaluations, and unfortunately accidents, one of which killed LT Thomas E. Selfridge, the Wrights modified their flyer. Finally, on 2 August 1909, the Army accepted the Wrights' airplane at a cost of $30,000 and designated it Signal Corps Aircraft No. 1.

Four years after the Signal Corps took charge of air matters, Congress appropriated specific funds for Army aviation in the amount of $125,000 for fiscal year 1912. By the close of October 1912, the Signal Corps had purchased 11 aircraft from the Wrights and their competitor Curtis Aircraft. These more powerful "scout" planes (Wright Type C) had been designed to

(Continued on page 12)

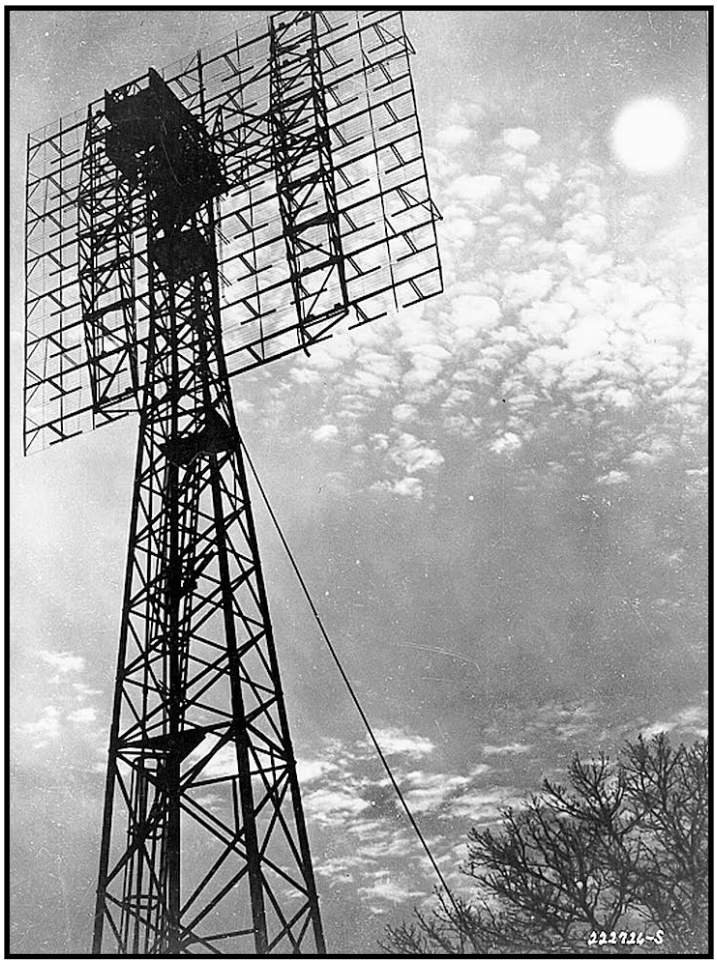


Photograph of Aircraft #5 of the 1st Aero Squadron during operations in Mexico in 1916. The aircraft were Curtiss JN4s, known as "Jenny's" and proved the value of aircraft for reconnaissance support for ground operations.

(Continued from page11)

perform reconnaissance and could carry radio and photographic equipment in addition to two men. Experimental activities during this time included night flying, aerial photography, use of the radio, and the testing of the Lewis machine gun from the air.

On 8 December 1913 the first U.S. aviation unit was activated, the 1st Aero Squadron (today the 1st Reconnaissance Squadron, U.S. Air Force). After the raid on Columbus, New Mexico by guerilla forces of Francisco "Pancho" Villa in 1916, the Signal Corps 1st Aero Squadron was deployed in combat operations to assist BG John J. Pershing with command and control during the Punitive Expedition into Mexico. During the expedition the 1st Aero Squadron flew 540 missions and illustrated how the air domain of warfare could be synchronized with ground operations, much as it had done with the navy during the Civil War.



Radar installation at Fort Monmouth N.J., juxtaposed against the moonlight sky to illustrate the accomplishment of bouncing communication signals through space.

From early work with balloons and the harnessing of powered flight, the Signal Corps served as the aviation center for U.S. military forces into World War I. As military aviation grew, many aviators such as BG William "Billy" Mitchell sought to separate themselves from Signal Corps control and gain an independent air organization. On 24 May 1918, President Woodrow Wilson created the Army Air Service organized directly under the War Department which officially ended responsibility for air matters by the U.S. Army Signal Corps. The Army Air Service thus became the forerunner of the U.S. Army Air Corps, the U.S. Army Air Force and in 1947, the U.S. Air Force.

Space Domain

The next domain the Army chose the Signal Corps to explore was determining the feasibility of leveraging outer-space for communications, particularly satellite platforms to extend the reach of military communications. On 10 January 1946, Signal Corps scientists, using a modified SCR-271 long range radar antenna succeeded in bouncing radar signals off the moon. Project Diana, named for the Roman goddess of the moon, demonstrated that very high frequency radio waves could penetrate the ionosphere encircling the earth and into space. After Project Diana, the Signal Corps broadened its space domain activities. In 1949, the Signal Corps provided electronic support for guided missiles, an effort which grew into the U.S. Army Signal Missile Support Agency. On 17 March 1958, a Vanguard rocket carried a satellite powered by solar cells developed by the Signal Corps Research and Development Laboratory at Fort Monmouth. The first communications satellite, Project SCORE (Signal Communications via Orbiting Relay Equipment), launched 18 December 1958 carried a Signal Corps-developed communications package. SCORE demonstrated that multiple voice and teletypewriter signals could be received, stored, and then retransmitted by an orbiting satellite. The Signal Corps mission for developing satellite payloads ended in 1962

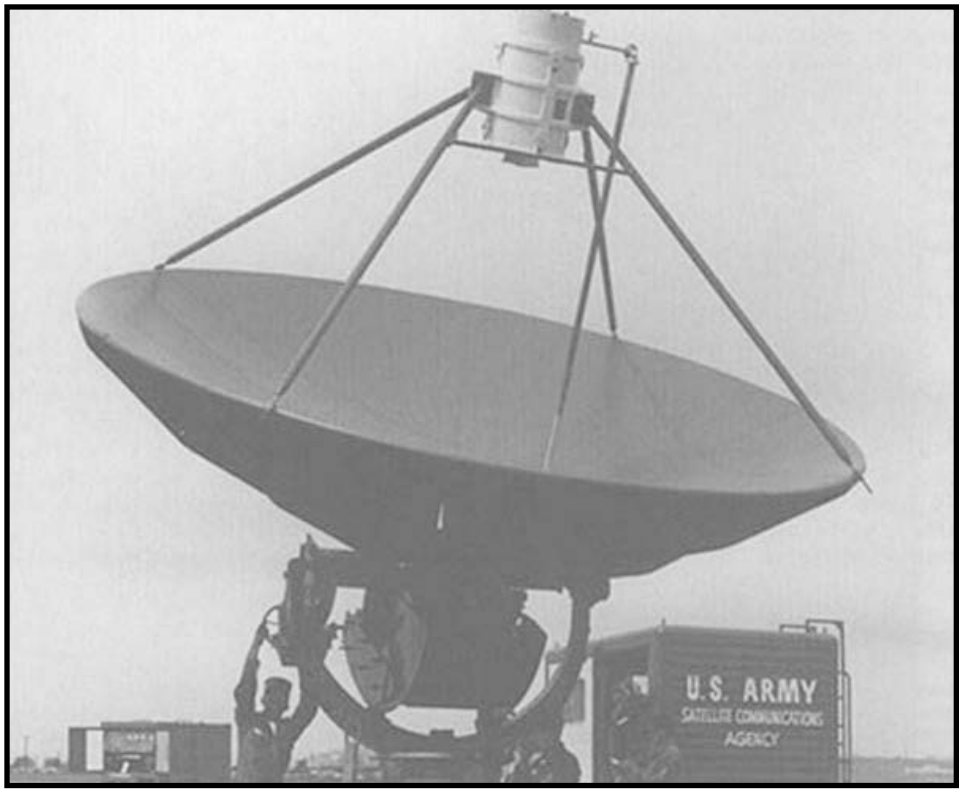
when the Army formed the Satellite Communications Agency, but that was only the beginning of using these platforms for warfare.

During the Vietnam War, the Signal Corps validated the use of satellites for providing integrated communications between land, sea, air and space domains. In August 1964, U.S. Army Signal Soldiers led by Warrant Officer Jack H. Inman established an experimental satellite ground station with one telephone and one teletype circuit to provide communications services between Saigon and Hawaii through a communications satellite 22,000 miles above the Pacific Ocean. This synchronous communications satellite system, named

Sign at Fort Monmouth, N.J., commemorating Project DIANA.

SYNCOM, was the first use of satellite communications in support of ongoing military operations. By October 1964, an upgraded SYNCOM provided one telephone and sixteen message circuits and proved that space-enabled communications could provide commanders with reliable and extended communications.

In 1966, GEN William C. Westmoreland, commander of Military Assistance Command, Vietnam, remarked, "The communications system . . . has responded brilliantly. No combat operation has been limited by lack of communications. The ingenuity, dedication, and professionalism of the communications personnel are deserving of the highest praise." Thus, the U.S. Army Signal Corps could add another domain to its resume of breaking new ground for communications in any sphere of operations, to include outside of the atmosphere of planet Earth.



U.S. Army Satellite Communications Agency satellite dish illustrating the capability of using space satellites to transmit signals over enormous distances in support of military communications.

Cyber Domain

Big decisions sometimes lead to big developments such as the Department of the Army decision in the mid-1980's to combine five information related functions into what was known as the Information Mission Area. The purpose of the IMA was to give commanders the information they needed more efficiently than before. The Signal Corps was assigned proponency for the functions of communications, automation, visual information, publications and printing, and records management. This decision soon resulted in renaming

(Continued on page 14)

(Continued from page13)

everything "communications" to "information" across the army. The Army Communications Command became the Army Information Systems Command and at the DA level, the Assistant Deputy Chief of Staff for Operations and Plans (Command, Control, Communications, and Computers) became the Assistant Chief of Staff for Information Management.

An important part of this process was the transfer of responsibility for the Army's computer science school from the Adjutant General School at Fort Benjamin Harrison, Ind., to the U.S. Army Signal School at Fort Gordon in 1988. This reflected the evolving concept of a desktop computer being a more efficient word processor to that of a unique communications platform for which information would be transported through an electronic, or cyber network. Now both the automation and communications proponency would be merged at one location under direction of the Signal Corps.

The mission for managing information technology saw its first test during Operations Desert Shield/Desert Storm in 1990-1991 in the sands of Saudi Arabia, Kuwait and Iraq. In addition to its traditional role of providing communications via radio, telephone and satellite this was a test for information transfer in the form of data, such as personnel, financial and logistics information via automation technology such as desktop computers.

This nascent information network also included the first in theater email system, which allowed deployed Soldiers to communicate with family members, thus linking commercial and military systems, which could handle up to 15,000 email messages a day.

After Desert Storm, Army leaders understood the potential of information technology systems to provide faster and more extensive information to provide real-time situational awareness in what was becoming a new domain of operations – cyberspace.

The result was the digitization of the tactical force, known as Force XXI. The 4th Infantry Division at Fort Hood, Texas, became the test bed for experiments using applied digital technology to combat systems, such as M1 Abrams, oriented toward obtaining information dominance over future adversaries. Digitization would also enable joint operations and the Army participated in fielding the Secret Internet Protocol Router Network, a classified network similar to the Internet for exchanging operational plans and information. The Non-Secure Internet Protocol Router Network was used to exchange less sensitive information. Together with the Joint Worldwide Intelligence Communications System, these networks comprised the Defense Information Systems Network.

Thus, information and communications "networks" began to merge resulting in another identity crisis for the Signal Corps as it faced challenges providing support during the Global War on Terror and the campaigns in Iraq and Afghanistan in the 2000s. These challenges took the form of what to call Signal units that provided this network of information technology systems. It began in 2002 when Department of the Army re-designated the 9th Army Signal Command as the U.S. Army Network Enterprise Technology Command/9th Army Signal Command with the authority to operate, manage, and defend the Army's "Infostructure"

at the enterprise level, consisting of command, control, communications, computers, and information technology services in support of warfighting forces. Thus NETCOM was born at the cost of de-emphazing its identity as a Signal unit.

This precedence set the stage for a 2007 identity crisis when the Commanding General of USAREUR wanted to change the designation of the 5th Army Signal Command to the 5th Theater Network Command to "better reflect all the missions that the unit accomplishes in today's Army." Fortunately, enough objections were raised by the Signal Corps leadership about the loss of the historical term "signal" and the ambiguity of the term "network" which could be applied to non-communications systems, such as logistics or transportation. Chief of Signal BG Jeff Foley was able to convince the Army CIO/G6 to reject this proposal arguing that a "Signal Command" conveys both the tactical and technical skills inherent in the duties of Signal Soldiers. This victory ensured the continuity of Signal Corps branch identity from the 19th to the 21st century would be maintained, at least until the next identity crisis occurred.

One may argue that crisis is upon the Signal Corps today. As the Army embarks upon determining its role in cyber space, where does that leave the Signal Corps? Will there be other initiatives that attack the rich heritage and history of one of the oldest and most capable branches of the U.S. Army? Will someone propose that Signal organizations be renamed "Cygnal," "Syber" or some other faddish term? Today, the Internet offers the ability to provide tremendous connectivity to every level of the force. The challenges of information security and reliability as well as control of the network must be achieved if the system is to be of use for military purposes. Cyberspace dominance must include the ability to operate reliably in the World Wide Web while possibly denying adversaries this ability. No other organization of the Army is capable of blazing a path into a new domain of warfare than the U.S. Army Signal Corps, which has repeatedly demonstrated though its history that it is the most experienced and capable to be given responsibility to overcome such challenges.

The challenges of information security and reliability as well as control of the network must be achieved if the system is to be of use for military purposes.

The Enduring Signal Corps

This short review illustrates that whatever domain of warfare it may be, the one enduring constant through 154 years of Signal Corps history has been the need for competent and dedicated Soldiers working in harmony with other armed services, to include international partners. Beginning with Albert J. Myers' vision of a group of technical specialists and leaders trained to provide communications capabilities, the men and women of the U.S. Army Signal Corps have consistently demonstrated they have the adaptive ability to function within the myriad spheres of warfare and dominate the battle space whether on land, sea, air or cyber domains. With each change in technology has come challenges but the Signal Corps historical record clearly demonstrates that it has provided reliable, rapid, and secure communications within any domain in which the U.S. Army finds itself facing confrontation from state or non-state opponents. More important than technology are the people – the men and women – the Soldiers and leaders – of the U.S. Army Signal Corps who have made success on the battlefields of American history possible. Whether by wig-wag or WIN-T--the men and women of the U.S. Army Signal Corps will continue ensuring that the message always gets through. Pro Patria Vigilans!

Steven J. Rauch *is the Signal Corps branch historian.*

WI-FI HITS THE BATTLEFIELD

By Amy Walker

Army technology is bringing the power of 4G to the battlefield so Soldiers can access mission information from their smartphones.

The 4G LTE infrastructure is part of a new collection of advanced commercial technologies, including coalition and first responder capabilities and Wi-Fi for command posts, that answer Soldiers' demands for tactical network systems delivering increased bandwidth and enhanced capabilities in smaller packages.

"Soldiers and commanders in tactical operations centers need more bandwidth for data intensive tasks like sending large PowerPoint files, maps, and full motion video," said LTC Joel Babbitt, product manager for Warfighter Information Network-Tactical Increment 1, which is responsible for fielding this new equipment. "The transformational nature of these technologies is increasing situational awareness and effectiveness for Soldiers at all echelons."

The Army fielded the Tactical Network Transmissions equipment package for the first time to the 86th Expeditionary Signal Battalion to support the Network Integration Evaluation 14.2 at Fort Bliss, Texas. NIE 14.2 was the seventh in the Army's series of semi-annual evaluations designed to integrate and mature the tactical network in a relevant operational environment.

(U.S. Army photo by Amy Walker)

Soldiers from the 86th Expeditionary Signal Battalion, B Company evaluated the new command post 4G LTE/Wi-Fi system (network stacks) at Army's Network Integration Evaluation 14.2 in Fort Bliss, Texas on May 7, 2014.

As their name suggests, the expeditionary nature of ESBs requires agility and advanced communications capabilities. These units are flexible and modular in nature, so they can support a vast range of missions in the most austere regions. They primarily support other units that don't have their own communications equipment. ESBs can support higher headquarters at corps and division, but they also have smaller teams to support units within a brigade combat team, or when needed, to provide network support for natural disaster relief efforts or other emergencies around the world.

The Army is providing the new TNT equipment collection to significantly increase network capability and throughput while reducing size, weight and power to help ESBs become leaner, more versatile and rapidly deployable. Some of the TNT equipment is also scheduled to be fielded to National Guard units for improved communications during civil support such as natural disasters.

Among the multiple capabilities provided by the TNT equipment is Wi-Fi coverage for the tactical operations center, removing some of the cables that tend to clutter command posts and allows Soldiers to roam from their desks so they can be more effective. In addition, a 4G LTE infrastructure, which covers the entire forward operating base, allows Soldiers to use their secure network on the battlefield via smartphones, and in the near future they will be able to use laptops and tablets with the capability as well.

"Commanders can just pick up their cell phones and directly call or text anyone they need to within the radius; it's a much faster line of communication," said CPL Michael Bullis, B company, 86th ESB, who operated the equipment at NIE 14.2. "On the software end, Soldiers have a centralized knowledge base on their phones, and the Army will continue to add apps to provide a more realistic view of what is going on in operations."

As part of the TNT effort, the Army married its 4G LTE/Wi-Fi system with a National Security Agency encryption solution, Commercial Solutions for Classified. It uses the same encryption technology as the commercial internet, enhanced for military purposes, enabling the Army to avoid research and development costs to incorporate this advanced technology. TNT is the first DoD program to utilize CSfC for military utility.

"Medics can use the 4G phones in forward operations, with apps like 'patient tickets,'" CPL Bullis said. "They put the information directly into their phone while they are right there on the scene, instead of having to come back, or give the information to someone over a radio to type it in."

The TNT technologies also include the Tropo Lite terminal, nick-named "Tropo in a can" by Soldiers because of its transit-cased deployability. Tropo Lite bounces microwaves off the atmosphere for high-speed transfer of large volumes of data between sites and over mountains – providing an alternative to expensive satellite communications.

TNT also includes a smaller, more transportable line-of-sight radio system called "TRILOS" that significantly increases throughput 12 times over legacy radios.

"Having more throughput means faster and more reliable services, and in wartime it is critical for a commander to send his message quickly,"

(Continued on page 18)

(U.S. Army photo by Amy Walker)

The Army's new Tactical Network Transmission equipment collection includes the new command post 4G LTE/Wi-Fi system (4G LTE/Wi-Fi antenna is seen left) and was evaluated at Army's Network Integration Evaluation 14.2 in Fort Bliss, Texas in May 2014.

(Continued from page 17)

said CPT Levelle Moore, B Company commander for the 86th ESB.

This spring's NIE included increased joint and coalition force participation, and to help support the coalition aspect of the event, the TNT package introduced the versatile Mission Network Enclave. This network stack can be rapidly reconfigured to provide tactical access for one of four different networks: the coalition network, Secure Internet Protocol Router, Non-secure Internet Protocol Router, or commercial internet and phone service. This flexibility enables MNE to support either coalition operations or civil support, such as first responders in disaster relief efforts. The system's integrated radio-bridging and cross-banding solutions provide seamless interoperability among disparate radio nets that previously could not communicate. The need for this type of capability was made evident by communication lapses such as those that occurred during Hurricane Katrina relief when first responders could not communicate between agencies.

"MNE is going to be great because we may be called to support a natural disaster or an emergency around the country, like Hurricane Katrina or Sandy," said MAJ Rickie Meers, operations officer (S3) for the 86th ESB. "MNE is going enable us to integrate all the different civilian agencies and combine all of their different radio systems and frequencies to be able to talk quickly between each of the agencies and with everyone out there. That is invaluable."

Along with increased capability, ease of use and SWaP reduction are high priorities for the Army, and Soldiers in the field are beginning to notice significant improvements as technology evolves. Before the turn of the century, electronic devices like televisions were large and cumbersome, and it took a lot of effort to move from location to location. But fast forward to 2014 and movies are being watched on smartphones and tablets. As technology continues to evolve, it's going to make missions easier on Soldiers and their units, Moore said. Additionally, today's Soldiers have grown up in a digital age and are often found teaching their parents how to operate new technology devices. The Army is working to make new technologies such as TNT more intuitive and easy to operate, which will also ease Soldier burden, he said.

"Soldiers are used to having some of this technology at home, so they just pick it up and can use it right away," CPL Moore said. "These new capabilities are going to be an asset in the long run and the Soldiers are excited about receiving this equipment."

Amy Walker *is a staff writer for Symbolic Systems, Inc. supporting the Army's Program Executive Office for Command, Control and Communications-Tactical; Project Manager Warfighter Information Network-Tactical and MilTech Solutions Office. She graduated from The College of New Jersey, Ewing, N.J. She has covered the Army's tactical network for six years, including multiple test and training events.*

Acronym QuickScan

CSfC - Commercial Solutions for Classified
ESB - Expeditionary Signal Battalion
LOS - Line-Of-Sight
MNE - Mission Network Enclave
NIE - Network Integration Evaluation
PdM - Product Manager
SIPR/NIPR - Secure Internet Protocol Router / Non-secure Internet Protocol Router
SWaP - Size, Weight and Power
TNT - Tactical Network Transmissions
WIN-T - Warfighter Information Network-Tactical

Command and General Staff College transforming Signal education

By Michael H. McMurphy and Gregory Thomas

Do Signal iron majors at the Command and General Staff College really have an opportunity to gain information assurance credentials?

The answer is yes.

The Signal Regiment's continuing professional partnership with the Department of Tactics-Command and General Staff College, is providing important educational opportunities for resident course signal officers.

The purpose of this article is to inform The Regiment on the professional relationship with the Department of Tactics, describe the intent of the credentialing opportunity, and to outline how a resident officer conducts their education and testing.

First, a description of the professional relationship will provide depth and breadth to the discussion.

The professional relationship between the 442d Signal Battalion and the Department of Tactics is significant. Twice a year, the commander of the 442d Signal Battalion is at Fort Leavenworth. Among the commanders many activities, dialogue with The Department of Tactics senior signal instructor is a high priority. The reason the commander coordinates with the senior signal instructor in the Department of Tactics is to provide commander's guidance. The senior signal instructor then generates suitable, feasible, and acceptable courses of action for new and/or better ways to provide educational opportunities to the resident signal student officers. Much of the dialogue includes feedback from prior student officers and input from senior signal leaders throughout The Regiment. The courses of action are then presented to the decision-making authority, the Director, Department of Army Tactics. His approval initiates a change to curriculum. The new curriculum is piloted during the winter-start CGSC class. After successful piloting, the new curriculum is fully implemented in the summer-start.

Simply put, we are executing mission command. Signal officers at the resident course provided the feedback and inspiration for a credentialing program. CGSC curriculum changes are then generated in a disciplined approach within the intent of the Director of Army Tactics and the commander, 442d Signal Battalion. The Director of Army Tactics is the decision maker. The 442d Signal Battalion provides suitable, feasible, and acceptable educational courses of action.

Providing these educational opportunities are important based on the facts facing The Regiment's iron majors in their pursuit of IA credentialing.

The most important fact is that a certified information systems security professional is an advance credential for IA workforce positions. Also, CISSP is the certification goal for all 25A Captain Career Course graduates. Although a goal, most graduates do not achieve it. Credentialing is self-study and not a part of the Institutional Domain of an officer's professional education. With these facts in mind, the intent behind the credentialing opportunity at Fort Leavenworth for resident students is significant.

The intent is to conduct certification at CGSC for our signal officers. If one were to ask "how can a resident CGSC student officer conduct self-study and gain a CISSP credential, yet also gain a letter grade for graduation requirements" then we have implemented a course of action that answers this question.

(Continued on page 20)

(Continued from page 19)

A short description of gaining a letter grade at CGSC for self-study will provide more clarity.

All officers attending resident CGSC are required to graduate with a minimum of 8 elective credits. The elective period for student officers is scheduled during their last few months of the resident course. The Department of Tactics offers a self-study elective listed in our CGSC catalogue as A309. Resident course signal iron majors can use A309 to gain a letter grade, for graduation requirements, through their CISSP self-study. Our CISSP program is identical to what some Engineer officers select to do at CGSC, i.e achieve their self-study professional credentialing: Project Management Professional.

The method of CISSP education and testing is very simple because everything is already in place. The systems for training, supervisor validation, and voucher requests are at Fort Gordon. We use the Fort Gordon Information Assurance Training Center webpage to conduct training.

First, the student officer coordinates with the senior signal instructor in the Department of Tactics. It is the most important step in the program. It ensures that the signal student officer executes their studies in a disciplined approach within the intent of the elective and their professional goals. Next, the officer conducts training on-line, using the Regiment's Skillport site.

Student officers complete their training modules and the pre-tests. The senior signal instructor uses the Army Training and Certification Tracking System to validate the training. Finally, the student officer requests a test voucher, the senior signal instructor validates the request on ATCTS, and the student officer receives a test voucher. The voucher can be used at any local TestVue center in the greater Kansas City area.

It conclusion, signal iron majors at the Command and General Staff College do have an opportunity to gain information assurance credentials. The professional relationship between the Regiment and the Department of Tactics has generated new curriculum for self-study while a signal student officer is assigned to the resident course. The systems for conducting the education, validating the education, and requesting test vouchers are already in place at Fort Gordon.

It's a better way to gain information assurance credentialing at CGSC

Michael McMurphy *is a retired Signal officer whose education and assignments include Ranger School, School of Advanced Military Studies, battalion and brigade S6, Signal battalion S3, and battalion command. Since 2006, he has been an assistant professor of tactics in the Department of Tactics, Command and General Staff College, where he also serves as the senior Signal instructor.*

Gregory Thomas *is a retired infantry officer whose education and assignments include, Ranger School, master parachutist, rifle battalion S3 and executive officer, and holds two master degrees. He is an assistant professor of tactics in the Department of Tactics, Command and General Staff College.*

Acronym QuickScan

TCTS - Army Training and Certification Tracking System

CGSC - Command and General Staff College

CISSP - Certified Information Systems Security Professional

PMP - Project Management Professional

Digital Master Gunner training keeping pace with latest technology

By Nancy Jones-Bonbrest

Think Geek Squad – only instead of driving Volkswagens and showing up in white short sleeves and clip-on ties, they're fully loaded and in charge of the most high-tech communications capabilities fielded by the Army.

Trained to operate, repair and troubleshoot the Army's network and mission command equipment, a growing number of certified subject matter experts are emerging to keep pace with the tremendous growth in digital information reaching across multiple systems.

Taking on this challenge to create experts for the Army, are Digital Master Gunner courses that are evolving to extend network capability training beyond Signal Soldiers to include noncommissioned officers, system integrators, operators and more.

"As systems become more integrated, these classes help us get the bigger picture of what we're trying to achieve on the battlefield," said SSG Daniel Beard, battle noncommissioned officer for the Tactical Operations Center with the 1st Brigade, 1st Infantry Division at Fort Riley, Kan. "I knew some of the systems that tie into the commander's TOC, but I wanted to know how all the systems link in with each other to get a better, overall picture of the operation."

This system-of-systems approach to Soldier training is crucial as the Army continues to field capability sets of integrated communications equipment to Brigade Combat Teams. Currently fielded to

(Continued on page 18)

(U.S. Army photo by Richard Bumgardner)

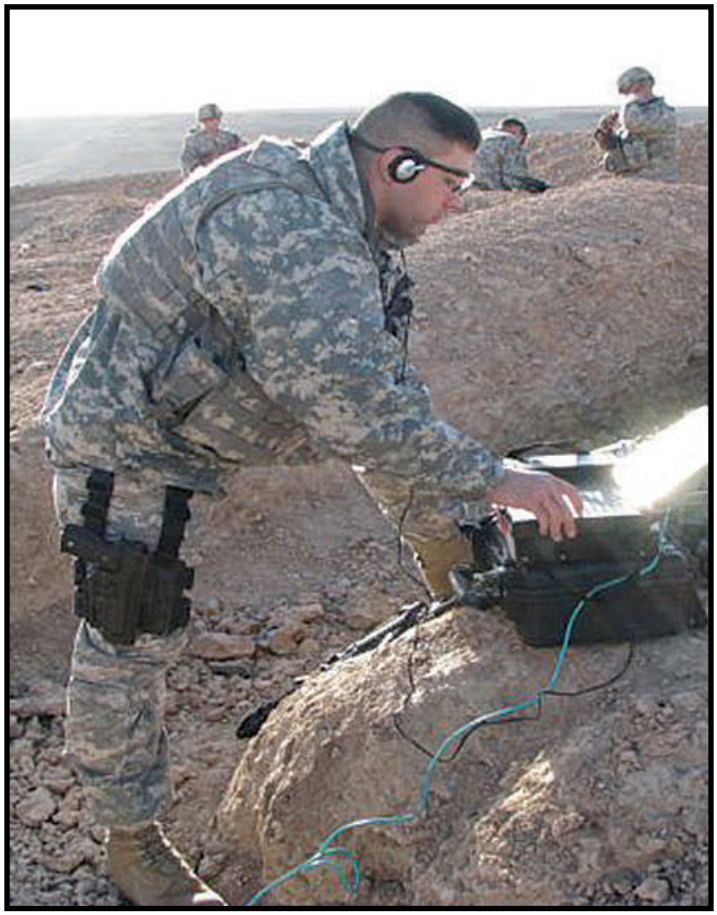
Digital Master Gunner courses offer a system-of-systems approach to Soldier training. This is crucial as Army planners continue fielding capability sets of integrated communications equipment to brigade combat teams. Digital Master Gunner courses look at the abilities of integrated mission command systems and how to build a common operating picture.

(Continued from page 21)

select BCTs deployed to Afghanistan, the newest technology is allowing Soldiers at all echelons to exchange voice and data from remote locations and across harsh terrain.

Focused on training for the latest capability set, the Mission Command Center of Excellence at Fort Leavenworth, Kan., currently offers two functional DMG training courses: a two-week Mission Command Digital Master Gunner Course and a three-week MC System Integration Course. The classes train Soldiers as subject matter experts on the Command Post of the Future, the Army's primary command and control system for TOC commanders.

"Our focus is on creating and maintaining one common operating picture for the commander," said MAJ Joshua Nolan, the Doctrine, Organization, Training and Strategy functional trainer for the MC CoE. "That's the bottom line, being able to pull all the systems in and create a good COP so the commander can make better, more informed, faster decisions on the battlefield."



(U.S. Army photo by Richard Bumgardner)

Capability sets have been developed and are being trained in Digital Master Gunner courses that are allowing Soldiers at all echelons to exchange voice and data from remote locations and across harsh terrain.

With a holistic look at the abilities of integrated mission command systems and how to build a COP, the courses show Soldiers what 'right' looks like so they can go back to their units and serve as the subject matter expert on digital operations. By establishing proficiency with the communications systems, Soldiers become the instructors.

"Before the classes, we would only see what the individual systems brought, but we knew that when we were able to combine the systems together, it gives us better situational awareness," said SSG Beard, whose unit went through a National Training Center rotation shortly after he completed both classes. "I was able to help younger Soldiers understand how the systems talk to each other and explain that you can determine what is going on with each individual warfighting function of CPOF without having to track down the individual people who input the data."

Last year, the two courses trained 353 Soldiers. This year they expect that to rise to more than 400.

DMG courses exist at installations across the U.S. and are established by many different organizations, including by the units themselves. The classes can also be brought to the unit, significantly reducing the time that Soldiers are pulled away from their duties.

The courses all share the common goals of training Soldiers to operate and maintain their own network and mission command systems, allowing the Army to keep pace with the rapid fielding of emerging network technology and at the same time offset the rightsizing of the field service representative contractor workforce. As retrograde from Afghanistan continues and military spending decreases, the Army is embracing a new field support

model that positions Soldiers as the first line of defense in troubleshooting command, control, communications, computers, intelligence, surveillance and reconnaissance equipment.

A five-week Signal-DMG course offered by the Field Support Branch of the Communications-Electronics Command at Fort Gordon, Ga., is focused on leveraging knowledge of each warfighting function and system that is part of the TOC. This includes instruction on power generation, the architecture of the Army's on-the-move network Warfighter Information Network-Tactical, satellite theory, CPOF and JCR-BFT.

"The Signal-DMG gives the Soldier the knowledge needed to take back to their unit and provide field support level training," said William Woodard, tactical communications integration team lead for CECOM's field support training. "We provide the Soldiers with all the training manuals, PowerPoints, and on-call support for questions to assist them with training the material to other Soldiers who weren't able to attend the class."

Last year 96 DMGs were trained through the CECOM course. This year that number is expected to grow to 160.

"This training includes detailed troubleshooting and a thorough understanding of the equipment to give the Soldier the knowledge needed to efficiently re-establish communications if an issue occurs," Woodward said. "The 'train-the-trainer' concept brings the knowledge and skills to the Soldier to increase the reliability and decrease the time to setup the equipment into a WIN-T network."

A three-week Cyber-DMG course, also developed by CECOM's Field Support Branch with the train-the-trainer approach, specializes in offensive cyber operations from a modern enemy perspective so Soldiers better understand how to protect their infrastructure. This course covers all information assurance tools available, with an emphasis on system hacking, session hijacking, web application vulnerabilities and risk management.

"Not only does this benefit the Soldier, but assists the Army with implementing cost-effective, high-quality training to help address the rapid influx of new technology," said James Hollingsworth, cybersecurity curriculum manager for CECOM's Training Support Division.

Last year 15 Soldiers went through the pilot Cyber-DMG course. This year they'll offer the class at four locations, with 64 Cyber warriors expected to graduate.

The Army will continue to utilize lessons-learned to evolve training methods that assist Soldiers in becoming better educated on network architecture and systems, allowing them to not only recognize when an issue occurs with a network capability, but to also be able to troubleshoot and adapt.

Nancy Jones-Bonbrest *is a staff writer for Symbolic Systems, Inc. supporting the Army Program Executive Office Command, Control and Communications-Tactical and MilTech Solutions. Jones-Bonbrest is a graduate of the University of Maryland, College Park.*

Acronym QuickScan

BCT - Brigade Combat Teams
BFT - Blue Force Tracking
C4ISR - Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance
CECOM - Communications-Electronics Command
COP - Common Operating Picture
CPOF - Command Post of the Future
DMG - Digital Master Gunner
DOT-S - Doctrine, Organization, Training and Strategy
FSR - Field Service Representative
MC - Mission Command
MC CoE - Mission Command Center of Excellence
TOC - Tactical Operations Center

Soldier input fuels network hotspot evolution

By Claire Heininger

The Soldier Network Extension is getting a mission makeover.

The SNE, which delivers the Army's mobile tactical network backbone to the company level, is evolving from a vehicle used by the company commander to an information hotspot allowing other Soldiers to plug in, make phone calls and send and receive data from anywhere on the battlefield -- from an Afghan polling place to an air assault observation point.

The changes, based on user feedback from Capability Set 13 fielded units and the Army's Network Integration Evaluation events, are also making the SNE more user-friendly through major reductions in startup and shutdown times, a simplified graphical interface and improved troubleshooting tools.

"That is going to be a game changer," said CPT Alexander Marotta, deputy communications officer (S6) for the 3rd Brigade Combat Team, 101st Airborne Division (Air Assault), which is currently training with CS 13. "Once we show people you can get into these things, hit start and all these systems will start up by themselves, that's where we're going to see more embracing of the systems. We're going to see the Soldiers want to use it."

The SNE is part of the Warfighter Information Network-Tactical Increment 2 mobile network that enables Soldiers operating in remote and challenging terrain to maintain voice, video and data communications while on the move.

WIN-T Increment 2 began fielding in October 2012 with CS 13, the Army's first integrated tactical communications package that provides connectivity across the BCT formation. Three CS 13-equipped units have since deployed to Afghanistan as Security Force Assistance Brigades, which work alongside Afghan forces as they improve their capabilities and assume responsibility for the security of their country.

Both the SNE and its battalion-level counterpart, the Point of Presence, were initially fielded on Mine Resistant Ambush Protected platforms that have been employed by SFAB units to support the U.S. advise-and-assist mission. Leaders say they are leveraging the PoP as the Army originally intended: to conduct mission command away from their command posts.

"It eased the transition between command post and mounted operations," said MAJ Gary Pickens, S6 for the 4th Brigade Combat Team, 10th Mountain Division (Light Infantry), which concluded its deployment in March. "In the past, when the commander gets in his vehicle, he goes from all of the capabilities in the command post to just an FM radio and Blue Force Tracking. With the PoP that didn't matter -- the key leader still had access to all of these different systems. To send updates at the tip of the spear through multiple different means was a capability they enjoyed."

The SNE, however, has filled a different role. Units say they use it less frequently as a company command vehicle, and more often as a mobile, ad-hoc network access point that provides reach back connectivity for multiple personnel. For example, during April's round of Afghan presidential elections, Soldiers from the 2nd Brigade Combat Team, 101st Airborne Division drove a SNE vehicle out to their assigned observation point near a polling place. There, they used the SNE to plug in multiple laptops for email, chat, and portal access, as well as to make Voice Over Internet Protocol satellite calls, allowing them to maintain full situational awareness of the election and associated security activities across the unit's area of operations.

The SFABs have also leveraged their SNEs to support information exchange in the coalition environment. The PoP vehicles were based on the U.S. component of the coalition network, which enables partner nations to share critical information and a common operating picture. Units then configured select SNE vehicles to use the Army's Secret

Internet Protocol Router Network, providing a U.S.-only communications capability as a complement to the PoP.

Back in the United States, the 3rd Brigade Combat Team, 101st Airborne Division this spring conducted Operation Golden Eagle, the Army's first brigade-size air assault mission since before 11 Sept 2001. While the Fort Campbell, Ky.-based training exercise did not warrant using PoPs and SNEs for their traditional mobile purpose, the unit positioned a SNE at a convoy staging area to provide the brigade's deputy commander with network connectivity to maintain situational awareness and send and receive reports.

"We did some very unique things with it," CPT Marotta said.

In addition to collecting insights and lessons-learned from the CS 13 BCTs, the Army is applying feedback from the 2nd Brigade Combat Team, 1st Armored Division, gathered over the course of several NIE field exercises at Fort Bliss, Texas, and White Sands Missile Range, N.M. The semi-annual NIEs provide Soldier input on the value of various network and mission command systems while helping to develop tactics, techniques and procedures for using communications equipment on the battlefield.

After using the SNE in a variety of operational scenarios, the brigade's leadership recommended that the SNE might not be the right match for a company commander, but because of its ability to enable critical Command and Control it should still be distributed at that echelon because it provides important connectivity to the upper tactical internet for access to full-motion video and other high-bandwidth information. In other words, they asked for the SNE to serve as a connection, not a tether.

"There is a debate right now on whether they need the SNE at the company level -- seeing how powerful it can be, my answer is yes," said COL Thomas Dorame, the commander of 2/1 AD. "(But) I want company commanders to be lean and capable to move, rapidly close and destroy, not overburden them."

SGT Martha Montes, a SNE operator in 2/1 AD, used the capability in a different role -- as a "retrans" link to extend the range of the brigade network for NIE. She said the real-time access to data and ability to make satellite phone calls increased the tempo of operations and improved Soldier safety.

"The people that are in combat can go farther out now since we have the retrans set up, so they will be able to talk to brigade," SGT Montes said. "That is why our job is so important. If we don't have comms, its over."

The NIE has also provided a test bed to evaluate WIN-T Increment 2 integrated on different platforms, such as Strykers and tracked vehicles. Strykers integrated with PoPs and SNEs are taking part in a developmental test at Fort Bliss this month, which will be followed by an evaluation with a full Stryker battalion during NIE 15.1 in October-November.

The Stryker assessment is just one part of NIE 15.1's Follow-on Operational Test and Evaluation for WIN-T Increment 2, which will also focus on validating the system changes to reduce complexity, increase reliability and reduce dependence on Signal Soldiers to operate and maintain the equipment.

These enhancements, coupled with operational insights about the SNE's evolving role, are expected to increase its utility on the battlefield for future CS fieldings.

"Soldiers deserve a network that is intuitive to operate and flexible to support their needs for various missions and formations," said LTC LaMont Hall, product manager for WIN-T Increment 2. "With their help, we will make sure we match the right capability to the right users, develop the right TTPs and continue to simplify the network, so it gives commanders and Soldiers the information they need but keeps their focus on the fight.

Claire Heininger *is a staff writer for Symbolic Systems, Inc. supporting the U.S. Army Program Executive Office Command, Control and Communications-Tactical. She is a graduate of the University of Notre Dame and a former statehouse reporter for the Star-Ledger, New Jersey's largest newspaper.*

LandWarNet Primer

By Patrick S. Baker

The LandWarNet is the U.S. Army's contribution to the Department of Defense Information Network.

The LWN is made up of all the globally interconnected communication and data transfer capabilities available to the Army.

One unique descriptor calls the LWN the end-to-end, foxhole to White House set of Army information processes. This includes all the personnel involved in collecting, processing, storing, disseminating, and managing all the information which supports war fighters' requirements.

The LWN includes all Army owned, leased and leveraged Department of Defense and Joint communications and computing systems and services. This includes software, applications, data security and other required network services.

The Navy and Marine equivalent of the LWN is FORCEnet. The Air Force equivalent to the LWN is the Command and Control Constellation.

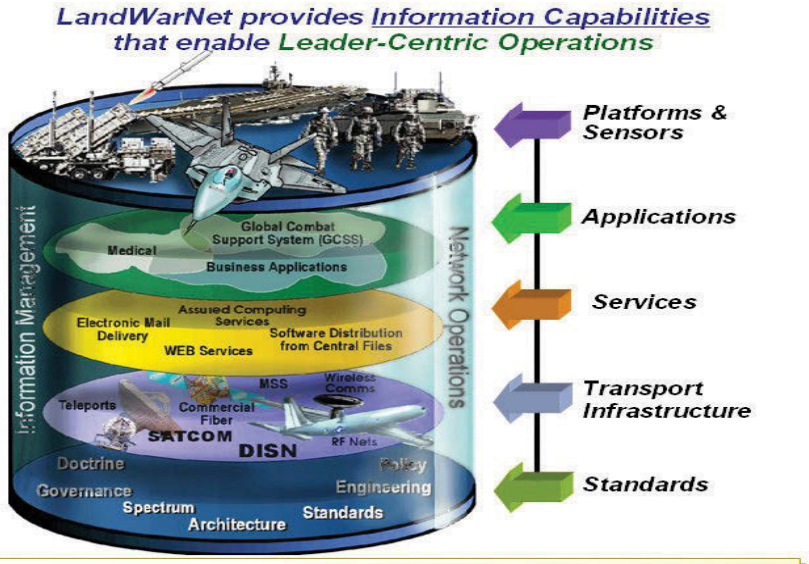
Mission Command

The LandWarNet enables and supports the Warfighter through the Mission Command (previously called Battle Command) concept. Mission Command is a technique of military command, which promotes relatively decentralized levels of command and control, providing freedom of action, and initiative, within certain constraints, such as the Rules of Engagement, and the commander's intent. Therefore subordinates, who understand the commander's intentions, have their own mission and the context of that mission within the larger framework of the operation, and are given very broad latitude on how to successfully complete the mission. Within Mission Command, concept orders are to provide only enough specifics to establish intent and objectives, and are to allow subordinate units maximum freedom of action.

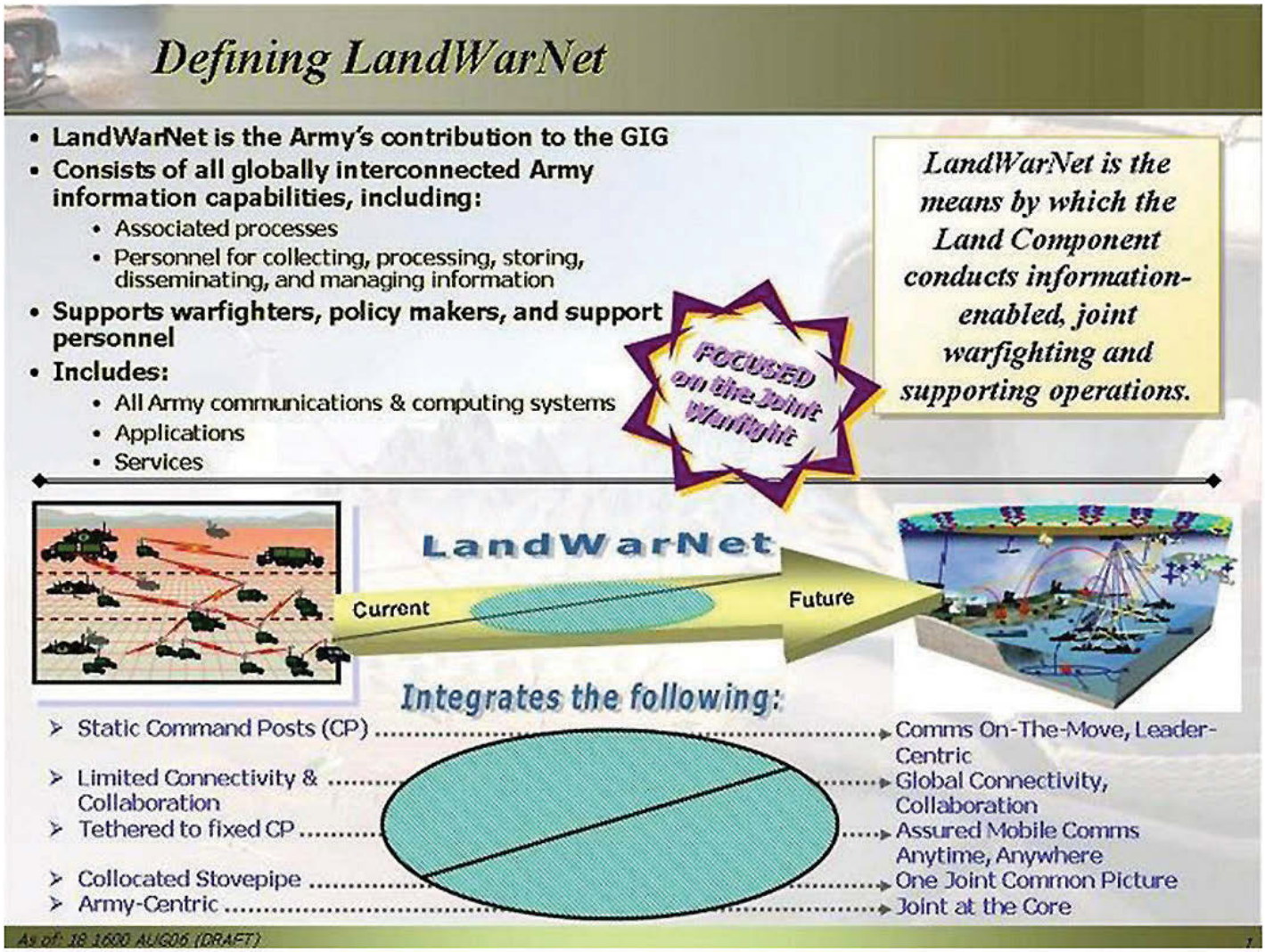
Modern Mission Command is enhanced by a decentralized approach to C2 in general.

LWN as key enabler

The Army's response to a generally decentralized command and control system is the LWN. The LWN is a key enabler for vital information at the point of critical decision making that assures full-spectrum dominance. Proper use of the LWN provides for quality information flow and speeds decision-making to enhance and support mission accomplishment. LWN integrates services and network transport across the Warfighting and intelligence domains to enable operations anytime, anywhere, at every echelon. LWN also creates unprecedented levels of flexibility and agility for support, intelligence, and situational awareness within Unified Land operations. The latest combat operations highlight the vital need for highly mobile land-based



The combination of what's on top and inside the cylinder = LandWarNet



communications, also highly mobile or long-ranged digital and voice networks, as well as satellite for communications over long ranges and across unfavorable terrain. Ultimately, LWN will be able deliver voice, data, and video to the tactical edge of formations across a geographically dispersed battle-space. It will push these capabilities to the lower echelons of brigades, battalions, companies and finally to the individual Soldier.

As the TRADOC Public Affairs Office once stated: "The Army's network capabilities will continue to emerge and mature. LandWarNet will capture these emerging capabilities, encompassing the evolving Mission command technologies, and link communications, information management and decision support."

Patrick S. Baker *serves as Analysic and Design Branch chief in the Directorate of Training at the U. S. Army Cyber Center of Excellence. He is a graduate of the Department of the Army Training Development Intern Program. He holds degrees in Education, History, European History and Political Science.*

ACRONYM QuickScan

C2 - Command and Control
DOD – Department of Defense
DoDIN - Department of Defense Information Network
LWN- LandWarNet
TRADOC – U. S. Army Training and Doctrine Command

CS-13 in combat

Adapting the network to the mission

By MAJ Graham Wood

The 3rd Brigade Combat Team, 10th Mountain Division (Light Infantry) was one of the first two brigade combat teams in the Army to field and deploy Capability Set–13, a suite of network tools designed to extend the network down to the Soldier level. This capability set represents a giant leap in terms of network capability and network extension beyond tactical operations centers.

However, there's one obstacle in the initial deployment. Nearly all these capabilities are tied to mine-resistant ambush protected vehicles. This posed a huge obstacle to 3 BCT's employment of CS-13 as we deployed to Afghanistan in a security force assistance brigade mission set.

Subsequently, this motivated our brigade S6 shop to develop several non-standard platforms, tailoring the network to fit the mission.

The components of CS-13 are divided into an upper tier and a lower tier. The upper tier is built around tactical communications nodes mounted on the family of medium tactical vehicles, the colorless core joint network node replacement. Additionally there are key leader vehicles: 48 MRAP all-terrain vehicles supporting points of presence, Soldier network extensions, and vehicle wireless packages capable of providing classified network access on the move by line of sight and satellite transmission.

The lower tier is comprised of networked Rifleman Radios and Nett Warrior End User Devices that provide position location information (situational awareness/command and control capability) displayed on a Motorola Atrix cell phone. While the lower tier systems are dismounted, they also require specially designed MATV's to link them into the global Blue Force Tracker network for messaging and position location information.

(U.S. Army photo by SGT Javier Amador)

CW2 Steven Hoxie operates the Lower Tier Internet Backpack during an advising mission in Khost Province, Afghanistan. This was the second operational test, from which a need for a new power solution was garnered.

This connection is provided through network services gateways that tie the Soldier Radio Waveform network into a 117G radio in a VRC-114 configuration, which then passes the Lower Tactical Internet data on to the vehicle mounted Unclassified JCR-BFT2, which completes the connection.

Of course the NSG package also relies upon the vehicle to supply power to all of these components. All told the upper and lower tier components of these vehicles weigh several hundred pounds.

Our brigade operated off of these mounted platforms for six months during our pre-deployment training. When we arrived in eastern Afghanistan with over 100 MATV based network platforms, we quickly discovered that in an SFAB mission set, nearly all of our troop movements were either dismounted to collocated Afghan bases, or rotary wing

inserted to remote Afghan bases. So there we were with the most sophisticated network fielded to any BCT in the Army, with a mission set that precluded its use.

The TCN's were integrated into the network at each of our six forward operating bases, providing redundant upper tier network connectivity to the robust microwave line of sight based network in Regional Command-East. The key leader vehicles were utilized far less, only supporting a single mission throughout the deployment, which was a retrograde from a company combat outpost, where the Soldier network extension vehicle performed spectacularly.

In this instance it provided classified network access up to the last minute and beyond as it was used to mission command the convoy movement off of the FOB. Despite this success, the upper tier simply did not fit the daily mission requirements in theater.

The Lower Tier systems aligned better with the mission set, providing dismounted networked voice capability along with BFT interoperable position location information and messaging.

The issue remained, however, that the full functionality of these systems relied upon a vehicle platform where advisors either flew or walked to work. Three BCT S6 shop had successfully dismounted all the components of the network services gateway onto a gator vehicle during its Joint Readiness Training Center rotation providing full lower tactical Internet functionality, so the concept of tailoring the network components to fit the mission started to gain a foothold.

Within the first month in Afghanistan our artillery battalion S6 shop replicated the JRTC gator, providing their advisors a network services gateway capable of insertion by a Chinook helicopter, and providing beyond line of sight position location information and messaging capabilities from collocated dismounted systems.

The system utilized the one kilowatt flex fuel generators provided with Nett Warrior to power the JCR-BFT2 TOC Kit and 117G Radio in SRW mode. Though still tied to a vehicle, the system can run upwards of 24 hours (fuel being the limiting factor), and provides the same network capabilities as the MATV platform.

This successful implementation of the CS-13 gator in combat highlighted the fact that the LTI capabilities did in fact align with the mission, if there was a willingness to alter the platforms that hosted the network.

The brigade S6 Lower Tactical Internet team tackled the next problem set by creating a TOC solution using transit case mounted radios at a coalition base to provide the NSG capability off of the existing power grid.

The brigade headquarters

(Continued on page 30)

(U.S. Army illustration courtesy 3rd Brigade Combat Team, 10th Mountain Division Public Affairs)

Dismounted blue feed icons from Nett Warrior systems displayed on a Blue Force Tracker system in a Tactical Operations Center in Paktika Province, Afghanistan, facilitated by the BFT Backpack; the Lower Tactical Internet systems also enable messaging between BFT and dismounted Nett Warriors.

(Continued from page 29)

is collocated alongside the Afghan National Army's 203rd Corps headquarters, where upwards of five advising teams walk to work to advise their counterparts on a daily basis. Given a 24-hour a day requirement and one vehicle per-radio network requirement, the use of LTI vehicles to support these daily advising missions was untenable.

Another issue was that each radio net requires a dedicated JCR-BFT2, of which the brigade only has a few running spares. Our LTI Technician engineered a non-standard solution with a Cisco switch to integrate up to five 117G radios, each hosting a different radio network, into a single BFT TOC kit.

This enabled position location information and messaging over to the ANA Corps area, but when advisors entered the Corps TOC they lost satellite feed for the PLI as well as the associated satellite timing that keeps all of the radios in sync with the network.

To mitigate the Global Positioning System issue the LTI team installed satellite repeaters into the plenum of the Corps TOC to maintain GPS lock for all advisors throughout the day. This non-standard solution, termed the walk to work solution, has become a staple of advising efforts at the 203rd Corps Headquarters. Nearly all advisors carry the Rifleman Radio for voice, also pushing their PLI to one another, to the Guardian Angel security teams, to the Base Defense Operations Center and the Brigade TOC, on both BFT and the Command Post of the Future.

(U.S. Army photo by SGT Javier Amador)

SFC **Joseph Caban, 4th Battalion, 25th Field Artillery Regiment S6 noncommissioned officer, tests the Lower Tier Internet Gator before its operational employment during an advising mission. The CS-13 Gator was later loaded onto a CH-47 Chinook for an advising mission in Khost Province, Afghanistan, the first non-standard use of CS-13 LTI in combat.**

It is a perfect example of tailoring the network to fit the mission, where the S6 shop was able to change how they operated to provide a system that fit the user's needs with a simple interface, despite considerable backside network complexity.

In the most recent installment of LTI adaptation, the 3 BCT S6 shop has taken the concept of the CS-13 Gator and downsized the NSG to fit within the medium rucksack. It weighs in at just over 50lbs, has a battery capacity of over 15 hours on two 5590 batteries and can be carried in a man-pack configuration or inserted now by a Blackhawk or Chinook helicopter.

The system is comprised of the same BFT TOC kit and 117G radio seen in the Gator, but with an ingenious power supply that uses 5590 batteries tied to a commercial off the shelf power inverter. This design finally detaches the NSG from the generator requirement. The system provides full NSG functionality in a man-portable package, the first solution that divorces the NSG from a vehicle of any kind.

The 3 BCT LTI team is still refining this system with the intent of reducing the weight closer to 35lbs, with a redesign

that facilitates its utilization while on the move. It is our hope to achieve this end state within our final two months in Afghanistan.

With each of these non-standard solutions, 3 BCT S6 shop has tailored components of a vehicle centric network to fit deployed requirements in a dismounted and air mobile SFAB mission set.

The true value in these systems is not necessarily the specific designs. These designs are not the panacea for future capability sets; rather they fit niche operational requirements that are equally susceptible to capability gaps like those identified in the vehicle platforms.

There is no single cookie cutter solution that can fit all foreseeable missions, but having adaptable components, and more importantly adaptable people that offer options is invaluable.

Distinct credit is due to CW2 Steven Hoxie, our LTI team lead and a 255A by trade, who has completely taken ownership of the CS-13 LTI, leading it in directions previously believed to be years away from development.

What is perhaps most impressive about all of these systems is the break from the reliance on field service representatives in CS-13. These systems were developed almost entirely by Soldiers with minimal assistance provided by a variety of civilian agencies, often remotely.

Lastly, each of these systems were developed not to just validate a signal capability, but to fill validated operational requirements in a combat environment.

For other brigade S6 shops fielding capability set equipment, I recommend applying this type of focus much earlier in CS training and utilization.

MAJ Graham Wood *is the brigade S6 for 3rd Brigade, 10th Mountain Division (Light), Fort Drum, N.Y., currently deployed to Eastern Afghanistan. His previous assignments include 21st Signal Company Commander (OEF IX) and 4-23rd Infantry Battalion S6 out of 2-2 SBCT at Fort Lewis, as well as 1-75th Cavalry Squadron S6 (OIF 5) and C/3-502nd Infantry Company Fire Support Officer (OIF 1) out of 2-101st Airborne at Fort Campbell, Ky.*

ACRONYM QuickScan

BCT – Brigade Combat Team
BDOC – Base Defense Operations Center
COP – Combat Outpost
CPOF – Command Post of the Future
CS-13 - Capability Set 2013
FMTV – Family of Medium Tactical Vehicles
FOB – Forward Operating Base
FSR – Field Support Representative
GPS – Global Positioning System
JCR-BFT2 – Joint Communications Release – Blue Force Tracker 2
JNN – Joint Network Node
JRTC – Joint Readiness Training Center
LTI – Lower Tactical Internet
MATV – All-Terrain Vehicle
MLOS – Microwave Line of Sight
MRAP - Mine Resistant Ambush Protected
NSG – Network Services Gateway
PLI – Position Location Information
POP – Point of Presence
RC-East – Regional Command East
RIP – Relief in Place
SA/C2 – Situational Awareness / Command and Control
SFAB – Security Forces Assistance Brigade
SNE – Soldier Network Extension
SRW – Soldier Radio Waveform
TOC – Tactical Operations Center
TCN – Tactical Communications Node
UTI – Upper Tactical Internet
VWP – Vehicle Wireless Package

COLLABORATIVE SPECTRUM MANAGEMENT

By SFC Nicholas A. Perez-Santalla

. The electromagnetic spectrum is a valuable resource that must be properly managed to benefit the military and society as a whole.

Spectrum governance in most regions of the world was established in the early twentieth century to accommodate government use. These legacy systems have failed to adequately adapt to the rapid rate of innovation in today's commercially dominated sector where we now have a proliferation of technologies vying for a position in a finite resource.

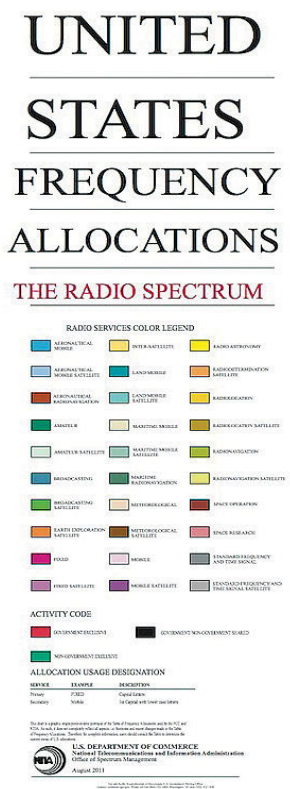
Over the past two decades, spectrum managers have begun reallocating spectrum use from government agency restricted to commercial uses because of shifting economic, political and strategic considerations.

These continuing shifts negatively impact agencies such as the Department of Defense operations and ultimately the national security environment of the United States, both at home and abroad.

Strategic and tactical operations require electronic spectrum domination to assure mission accomplishment. Reallocating spectrum resources from federal agencies, especially the DoD, will negatively impact our ability to meet the political objectives of the United States. Vacating the DoD of currently occupied spectrum bands creates a need for the DoD to spend an enormous amount of money investing in new systems, modifying the current systems and training personnel on new technologies and systems.

Disclaimer

The opinions and conclusions expressed here are those of the author and do not necessarily represent the views of the National Defense University, The Department of Defense or any other governmental entity. References to this study should include the foregoing statement.



Antiquated command-and-control governance and utilization of the spectrum must end. A framework for a more collaborative approach is required to successfully meet the needs of both the federal government within the national security environment and commercial industries.

DOD Reallocation Efforts

In order to maintain communications domination, war fighters require worldwide, on-demand spectrum access. We can see from recent operations in Iraq and Afghanistan that the ability for a commander to project force is dependent on the ability to exploit technology. Historically, this has not been an issue.

Yet, today, with the emergence of new technologies, the demand from both federal and commercial consumers, transitioning to wireless infrastructures, has obstructed the DoD's ability to navigate freely in the utilization of this resource both at home and internationally.

In a slow-changing regulatory and administrative atmosphere, U.S. spectrum policy has become a dynamic environment for all stakeholders demanding more access to resources. Realizing the positive economic impact of federal reallocation, government officials systematically call for reallocation from federal users, primarily the DoD, as far back as 1993. The Omnibus Budget Reconciliation Act of 1993 reallocated 235 MHz of federal allocated spectrum to be auctioned off to the private sector (Congress 1993). Four years later, in the Balanced Budget Act of 1997, an additional 20 MHz of federal spectrum was called to be transferred to the Federal Communications Commission for reallocation.

In 2002, the FCC formed the Spectrum Policy Task Force to help with identifying and evaluating changes in spectrum policy. This commission was tasked with providing guidance in making spectrum regulation more market-oriented, moving towards unlicensed device or commons models, and minimizing regulatory intervention. In November 2002, the SPTF released a report that recommended moving certain parts of the spectrum from a command-and-control infrastructure to both unlicensed and licensed flexible-use policies.

In June of 2010, President Barak Obama released a memorandum stating that, "America's future competitiveness and global technology leadership depend, in part, upon the availability of additional spectrum." He continued to call for the FCC and the National Telecommunications and Information Administration to release a plan to free up 500 MHz of spectrum for commercial use in the next 10 years. This memorandum states that the ability to communicate is not the only utility of spectrum. Governance of this resource directly affects the economic strength and stability of the nation via the U.S. wireless industry. In May 2012, in response to the Presidential memorandum, a report was released detailing the relationship of spectrum to the economy through empirical data.

The report states that if an additional 500 MHz of spectrum could become available for commercial use over the next ten years, it could mean an increase of $166 billion for U.S. gross domestic product, and boost economic revenues to $36.7 billion. Also, the wireless industry was responsible for 3.8 million jobs as of 2011, which was an increase of 200,000 over the previous six years, accounting for 2.6% of all U.S. employment. The implications of both the Presidential memorandum and the empirical analysis legitimize the importance of proper governance mechanisms controlling spectrum in the United States.

2014 Spectrum Strategy

In February 2014, DoD Chief Information Officer, Terri Takai, released the latest DoD strategy for addressing the demand for spectrum access, specifically as it applies to achieving national security goals. *Electromagnetic Spectrum*

(Continued on page 34)

(Continued from page 33)

Strategy: A Call to Action sets short-term and long-term goals for the DoD.

Analysis of this strategy finds, through consideration of the language used and priorities presented, that the DoD may be prepared to vacate the 500 MHz of spectrum as laid out in the President's direction of 2010, but would prefer not to lose any current capabilities. Analysis of this latest strategy finds that the DoD is providing an alternative solution by advocating a type of commons governance approach for future operation of spectrum. For example, throughout this research project, the National Military Strategy is often referenced as saying, "The Joint Force must ensure access, freedom of maneuver, and the ability to project power globally through all domains," and it specifies these domains as land, air, sea, space and cyberspace.

The latest DoD Spectrum Strategy also makes this reference and raises a point often overlooked by federal authorities – that is, spectrum transcends all of these domains. The access to spectrum is a force multiplier, and the denial of spectrum to the enemy is of significant importance to battle space superiority. Essentially, the DoD is placing spectrum, and access to it, as a priority over all other domains – a perspective that is not often shared by regulators and administrative offices.

With the release of this strategy, the DoD is making yet another attempt to educate regulators on the critical importance of accessing spectrum when needed to ensure that the United States is both capable and ready to defend and protect the nation against all threats and quickly secure and maintain information superiority no matter what the future of conflict or stability operations may hold.

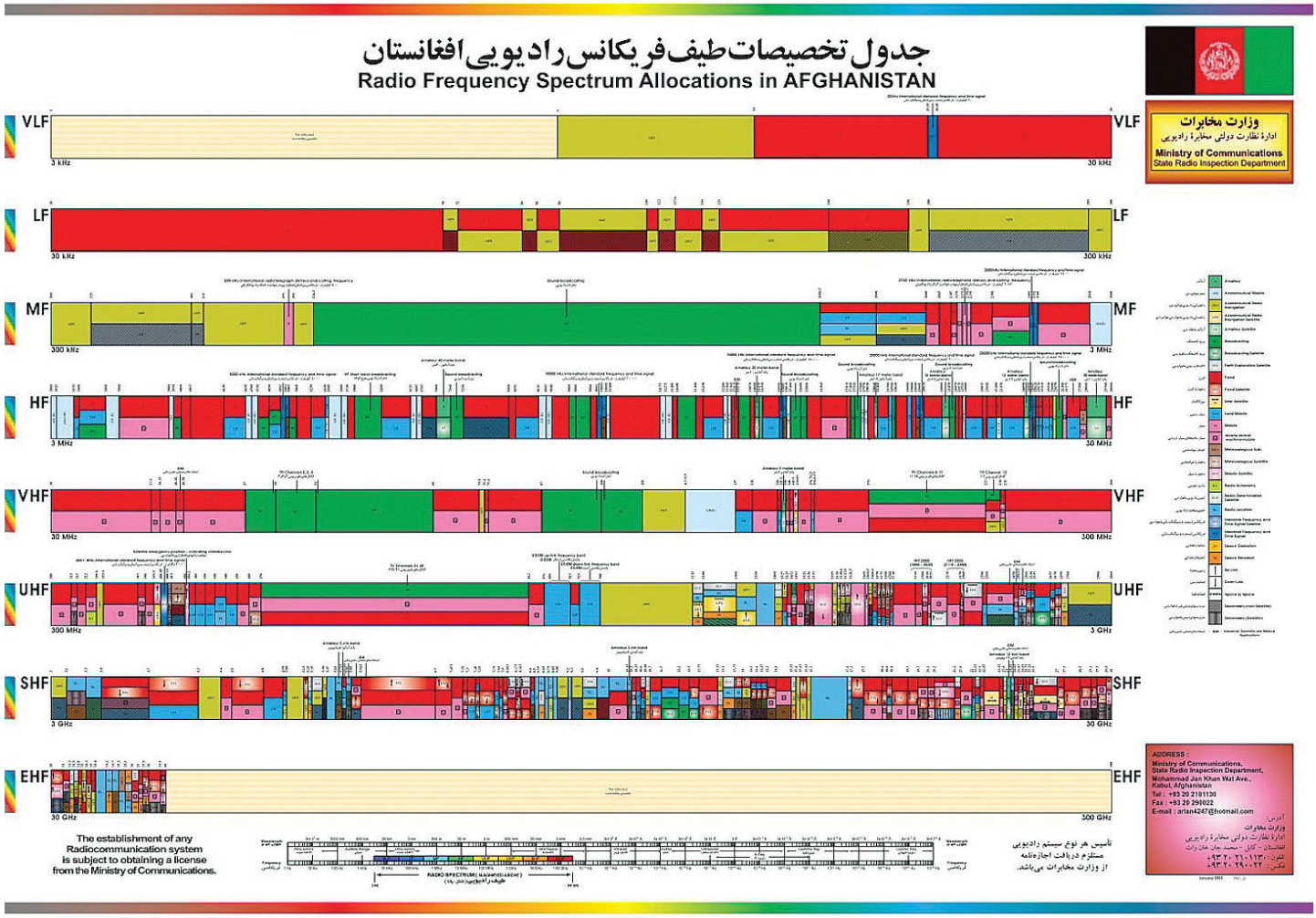
This strategy seems to be more of a mission statement and less of a plan. The DoD has set forth a number of goals and objectives to actively monitor and be involved with spectrum changes both operationally and administratively in this document; however, the tools required to do so are still being developed as the document states that, "A Roadmap and Action Plan will be developed to supplement this strategy."

The DoD has realized that a more involved role in discussions concerning regulation both domestically and internationally will allow the department to shape the allocations of and thinking about spectrum both now and in the future. The DoD can no longer deal with reallocation, and will experience a severe impact to current and future operations--combat or peacekeeping, if the current regulatory processes continue unchanged. Collective action seems to be almost required in investigating possible solutions to supporting both DoD and commercial needs for access to spectrum.

Afghanistan: A Missed Opportunity

As an example, Afghanistan has begun selling sections of spectrum through licenses to technology developers, preventing U.S. and coalition forces from operating in critical spectrum that is required to sustain both combat and support missions in the country. While respecting Afghanistan's requirement to bolster their economy through revenue received from spectrum licensing fees, the United States should also encourage the Afghan Ministry of Communications and the Afghanistan Telecom Regulatory Authority towards a common regime of spectrum governance, given the current state of the nation's technological infrastructure and the opportunity to spread allocation out geographically.

While the United States has been relatively successful with status quo regulatory mechanisms it is easily conjectured that change is necessary. Afghanistan operations offer a clear example. Afghanistan will certainly experience the same issues of resource scarcity and congestion that the United States is experiencing today if progress towards a more technologically friendly environment is not anticipated and managed. As regulators in Afghanistan begin to fully understand the importance of this resource, they will also continue to realize



its monetary value and begin reallocating it from central government to commercial industries.

The United States, through Afghanistan, should have taken the opportunity to utilize Afghanistan as a proof of concept for shared space. In my opinion, Afghanistan spectrum development reflects a failed opportunity to test and develop a spectrum governance environment that the United States could have managed and validated for ground-up design of a total system for possible use in the United States. Not only would the United States have been able to mitigate threat but also demonstrate on a global scale that a shared environment is a possibility and thereby take important steps toward harmonizing spectrum regulation worldwide.

Also, through investing in Afghanistan's infrastructure based on a wireless foundation, instead of terrestrial, the United States and coalition forces could have enhanced Afghanistan's regional presence by establishing them as a leader of technology in the region. Trained in the antiquated processes of the United States, the ATRA and Ministry of Communications in Afghanistan have already started to push the DoD out of the critical spectrum needed to conduct combat and stability operations.

This is a delicate situation and a problem that is on one hand, beneficial to the sovereignty and ability of the nation of Afghanistan to regulate within its borders, and on the other hand, detrimental to continuing operations for both the United States and coalition forces. If Afghanistan leaders continue developing the technological infrastructure,

(Continued on page 36)

(Continued from page 35)

then they are certainly destined to experience the same resource scarcity and possible negative impacts to their national security environment. Understanding this reality and developing Afghanistan as a leader in spectrum efficiency and technology development overall, will heighten its presence as a regional power in the Middle East and invite corporations and other governments to invest in the nation's stability and success.

Recommendations and Conclusion

Increased dependence on spectrum will only continue and regulators need to understand the impacts to the both the economy and national security environments if reallocation from DoD continues in the future. A common regime of governance will support both the commercial industry and federal agencies, primarily the DoD, for accessing spectrum when and where required . The federal government and FCC will still have a role to play, a role by setting technological standards for equipment that can operate in a given spectrum band – standards that promote efficiency and occupy the least amount of spectrum to conduct operations, whether those operations are for commercial companies or the DoD.

Investing in technology and aggressively developing existing technologies can serve as a partial solution to spectrum scarcity and, by extension, reallocation efforts. For example, transitioning from fixed-frequency transmissions to spread spectrum technology. Spread spectrum is not a new technology; however, development within spread spectrum is advancing rapidly. Spread spectrum systems are adaptable; they allow for a signal to be intentionally distributed over a large portion of spectrum. Spread spectrum systems utilize a variety of other technologies to achieve these means, including frequency and time hopping and utilization of code to distribute transmissions through Code Division Multiple Access.

Cognitive radio, another promising technology that has been recently developed, accesses spectrum opportunistically. The system detects unused spectrum in a licensed band and operates within it. Once the incumbent transmission is detected, it will vacate that spectrum, thereby eliminating the possibility of interference, and making it possible for multiple users to occupy the same spectrum. Cognitive radio also utilizes technology such as Software-Defined Radio, where traditional hardware components of a system are replaced with software. This dynamic process allows for updating and modification of signal processing. Instead of expensive hardware modifications or investing in totally new systems, SDR can enable the DoD and commercial industry to manipulate signals more efficiently as technology becomes available.

These are only a few examples of how the advancement of technology and systems can overcome the perceived problem of spectrum scarcity. The interference that users receive or are responsible for is a product of the technology that they use, not the spectrum itself. Focusing on technologies that are more efficient for all spectrum stakeholders is vital for the creation of "more" resource.

Technology is relative. Through the development of new technologies, access to spectrum can change. Regulation of spectrum was created out of necessity. As Eli Noam stated in an article for *Telecommunications Policy,* "Change the technology and the economics and the law of spectrum use must change too." Once it has been demonstrated that a common environment is possible, regulation and policy will begin to change. The DoD cannot continue relinquishing spectrum for the stimulus of the U.S. economy.

While the DoD is not going to pay for spectrum access like commerical industries, there will have to be collaboration in the development of new technologies that allow for shared access to this resource.

Dynamic spectrum access and spread spectrum technologies are only partial solutions here. Spread spectrum technologies

support the argument that spectrum scarcity, like technology, is a realative issue. It is because of spectrum scarcity that reallocation efforts are being taken. As these technologies develop and the risk for harmful interference diminishes, regulatory authorities will be more receptive to policy change.

There is no easy solution to this problem. The DoD is continually being called upon to relinquish spectrum allocations to the FCC for auction to commercial entities. Technology is certainly a partial solution. Private companies are developing technologies that efficiently utilize spectrum. Accordingly, it would be wise for the DoD to be part of that development so that everyone is looking for more efficient utilization. As outlined in their most recent Spectrum Strategy, the DoD understands that participation on every level of regulation and the development of technologies will give them a louder voice in discussions.

While the DoD's access to spectrum on-demand is of critical importance to national defense, that argument is often reactionary and will not deter future reallocation efforts.

Changing the governance regime in the United States is an impractical solution, but changing the historical predispositions on spectrum and the possibilities of common usage can alter the current landscape for both commercial industry and national defense. The DoD is both the federal government's greatest occupier of spectrum and the department most capable of understanding and efficiently utilizing this resource effectively. While auctioning off more spectrum may be more beneficial for collecting revenue to counter the national deficit, no dollar amount can be placed on the importance of the DoD's ability to meet national security objectives, maintain a technological edge over any current or future adversary, and also drive future capabilities and spectrum access requirements of our allies through technology.

Defense outweighs monetary stimulus with respect to spectrum access. Risking the DoD's ability to defend U.S. interests should be avoided at all costs. Diminishing capability through antiquated regulatory process and spectrum reallocation hurts both training and operational capability for the DoD to succeed in its mission of supporting national security objectives.

Creating an environment that fosters a collaborative effort to create technologies that will encourage and allow simultaneous use of the same spectrum is critically important to reducing the necessity for reallocation while servicing the needs of both the commercial and defense industries.

SFC Nicholas A. Perez-Santalla *is a recent graduate of the National Defense University's Master of Arts in Strategic Security Studies program at Fort Bragg, N.C. He is an active duty 25E, electromagnetic spectrum manager, with multiple operational tours in the CENTCOM AOR. He is a 12-year veteran of the Signal Corps, before reclassifying to 25E in 2010; he served as a 25L, cable systems installer maintainer.*

Join the Discussion

https://SIGKN.army.mil

Acronym QuickScan

ATRA - Afghanistan Telecom Regulatory Authority
CDMA – Code Division Multiple Access
CIO - Chief Information Officer
CR – Cognitive Radio
DoD - Department of Defense
FCC – Federal Communications Commission
GDP – Gross Domestic Product
NMS – National Military Strategy
NTIA – National Telecommunications and Information Administration
SDR – Software Defined Radio
SPTF – Spectrum Policy Task Force

Sharing the electromagnetic spectrum

By CPT Bryant A. Wellman
and CW5 Garth R. Hahn

Spectrum sharing has gained national level attention as a way of furthering the economic exploitation of spectrum resources while protecting national security interests.

The electromagnetic spectrum is the medium that mobile phones, satellite communication systems, garage door openers, RADAR, and Wi-Fi devices operate within to send and receive information wirelessly.

It is not only important to our military forces and federal agencies, but an economically critical resource used by commercial companies around the world. It is this friction point that must be balanced at the national level to ensure adequate spectrum access for our forces to train on battlefield systems in the United States, while enabling the quickly developing market for mobile data to expand and innovate.

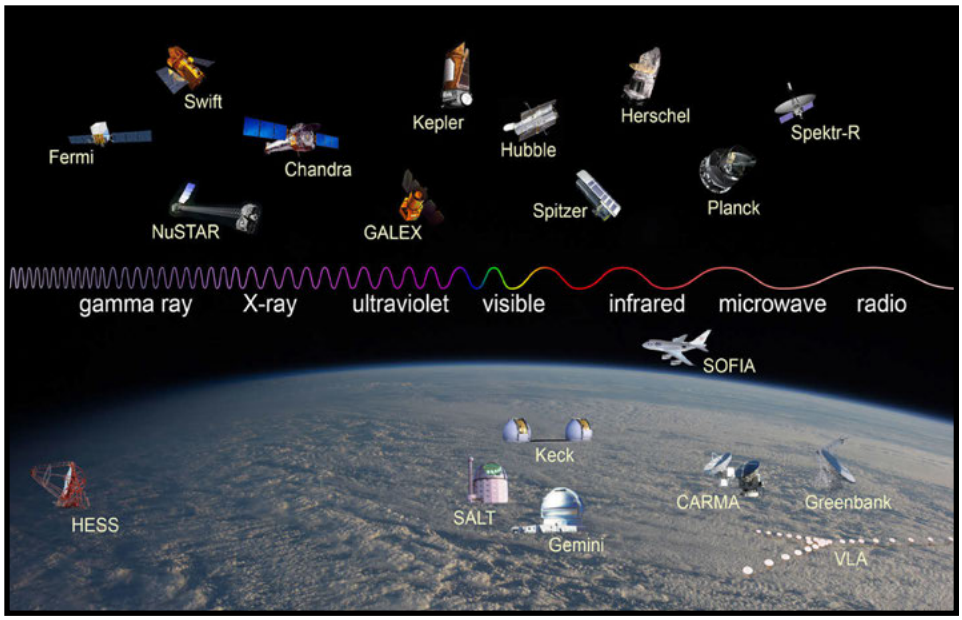
In an increasingly crowded space, spectrum sharing is emerging as one method to enable our forces and our nation's commercial needs to coexist.

Federal spectrum management dates to the 1920s when radio broadcasts by federal and commercial stations and the subsequent interference between those stations, demonstrated a need for management of the resource.

Today, there are two agencies at the federal level that manage spectrum policy in the United States, the National Telecommunications and Information Administration and the Federal Communications Commission. The NTIA was established by executive order, and operates under the Secretary of Commerce to govern all radio transmissions made by U. S. Government stations. The Federal Communications Commission was established by The Communications Act of 1934, and is responsible for regulating non-federal transmissions. Together, these entities provide spectrum management of all radio transmissions in the United States. These rules and regulations are codified in the Manual of Regulations and Procedures for Federal Radio Frequency Management – commonly called the "Red Book", which is published and updated by NTIA, and the Code of Federal Regulations Title 47 – Telecommunications, which are the rules created and managed by the FCC. At the international level, the International Telecommunications Union establishes rules for areas outside of the territorial limits of individual nations, and other nations establish their own rules for radio frequency operations within their borders.

Over time, the FCC and the NTIA developed bands of federal and non-federal allocated spectrum that allowed each agency to assign spectrum to their stakeholders, with minimal coordination. This spectrum segregation can most easily be seen in the Table of Frequency Allocations, in the NTIA Red Book Chapter 4, or the CFR Title 47, Part 2. The table has an international column (the U.S. is in Region 2), and a U. S. column, which is further split into two other columns signifying federal and non-federal tables. Instances where both of the columns indicate allocated radio-communication services identify shared spectrum, and frequency use in this band must be coordinated between the FCC and NTIA.

Modifications to the Allocation Table are made by NTIA with recommendations from the Interdepartmental Radio Advisory Committee, which is chaired by NTIA and



attended by a FCC liaison, and/or the issuance of a Report and Order by the FCC modifying the Code of Federal Regulations.

In recent years, there has been pressure placed upon national regulators to open up new spectrum for commercial use. In 2010, the White House released a Presidential Memorandum titled "Unleashing the Wireless Broadband Revolution", which requires federal agencies to make 500 MHz of spectrum available for commercial use within 10 years.

In July 2012, the President's Council of Advisors on Science and Technology issued a report concluding that "clearing government-held spectrum of Federal users and auctioning it for commercial use is not sustainable," and urges the President to direct spectrum sharing to meet the need for commercial bandwidth. Finally, in June 2013, The White House released the Presidential Memorandum entitled "Expanding America's Leadership in Wireless Innovation."

This memorandum states that "sharing can and should be used to enhance efficiency among all users and expedite commercial access to additional spectrum bands." These three documents attempt to address the shortfall of available spectrum needed for continued wireless commercial systems by opening up federal bands to sharing with commercial systems.

The explosion of wireless systems in the last five years has created a critical need for more bandwidth to support the public's expanding desire for spectrum dependent systems such as tablets, smartphones, WI-FI access points, and a host of new technologies that will allow vehicles, home appliances and heating/cooling systems and other items, collectively known as the internet of things, to operate.

This boom in wireless systems comes as technological means of passing more information over spectrum is bumping up against Shannon's Law. This law, written by engineer Claude Shannon in 1948, and outlined in the article "Shannon's Specter" by Kevin Fitchard, states that "the amount of error-free data that could be transmitted over a channel of any given bandwidth is limited by noise." The wireless industry has evolved their system's efficiency to pass more data over the same amount of spectrum, but has reached a level of efficiency that will require more spectrum to continue to expand download and upload speeds of wireless devices. This additional spectrum may well come through the sharing of existing government bands within which the Department of Defense operates.

A recent agreement on the 1755 – 1780 MHz band will result in the Department of Defense and other federal users clearing from that spectrum and relocating. The FCC will then auction this band as part of the Advanced Wireless Services

(Continued on page 40)

(Continued from page 39)

auction. However, this clearing and moving is an expensive proposition for federal spectrum users. Cost estimates of moving all operations out of this band and relocating to another run to $3.5 billion. To avoid the expense of future clearing of federal spectrum, the sharing model, proposed by the PCAST report and embraced by the June 2013 Presidential Memorandum, will enable new entrants to existing federal spectrum while protecting the operation of the incumbent federal systems.

Spectrum sharing between federal and non-federal users is not a new concept, and a short review of the National Table of Frequency Allocations will show many bands that are allocated to both types of use. Additionally, within various allocations federal users share the spectrum with other federal users, and non-federal with other non-federal users.

The bottom line of sharing spectrum is that, typically, it is not physically possible to share the same discreet frequency at the same time and geographic location. Therefore sharing is now accomplished by creating exclusion zones around users geographically to protect their spectrum usage according to the power and modulation of their signal.

What is new about spectrum sharing is that our ability to dynamically identify spectrum use through technical methods like dynamic frequency selection, cognitive radio and geo-location, spectrum managing databases will allow different types of services to share the same spectrum bands in real-time while avoiding harmful interference between operations. While each of these technologies has challenges, these and future, yet-to-be-developed technologies lay the groundwork for real-time, massively shared spectrum. To that end, there are two bands that are currently under review for sharing between federal and non-federal users, 3550-3650 MHz and portions of the 5 GHz bands.

The 3550-3650 MHz band is currently used by federal stations for Radiolocation Service and Aeronautical Radionavigation Service (ground based), and by non-federal stations in the Fixed Satellite Service.

In the Notice of Proposed Rulemaking and Order, FCC 12-148, released in December 2012, the FCC proposed modifying the use of the band to include both licensed and unlicensed devices (think cell phones and WI-FI) across this band, while protecting the incumbent users, primarily federal radar use by the Navy, and Fixed Satellite use by commercial organizations. In their Fast Track report, in response to the Presidential Memorandum regarding spectrum sharing, the NTIA identified the band 3550-3650 MHz as a potential band that could be shared with commercial users.

The FCC added 50 MHz, 3650-3700 MHz to consideration in its proposed rulemaking. This band has a low propagation characteristic, meaning its range is less than for signals at lower frequency ranges. According to the NPRM, this characteristic makes it "well-suited to spectrum sharing, particularly geographic sharing". This sharing would be facilitated by the lower propagation of signals in the band, which makes it suitable for small cells.

The NPRM identified a multi-tiered licensing and interference protection framework to three types of users, or tiers, "Incumbent Access, which would include authorized federal and grandfathered FSS users." Priority Access would include users with a quality-of-service requirement. Finally, the General Authorized Access would consist of users with an opportunistic access to the spectrum. Each tier would get interference protection from the next lower tier, from Incumbent to PA to GAA. This interference protection would come from a Spectrum Access System.

The SAS would govern interactions between the tiers within the band. PA and GAA users may be silenced, or limited in operating power or geographic operating location when an incumbent comes up for operation, and the GAA will be required not to interfere when it operates. This design builds upon the Television White

Space program, which uses databases to enable sharing of bandwidth cleared when digital television stations replaced analog stations. However, the SAS envisioned for use in the 3.5 GHz band is much more dynamic and therefore a more complex system.

The rules on how this band will ultimately be used are still being written, and collaboration between NTIA and the FCC is ongoing, but there is an emerging value in this sharing model for the U.S. Army. As the allocation tables are modified to allow federal and non-federal sharing in the 3.5 GHz band, there will be opportunities for the Army to obtain commercially created communication systems for high-speed data transfer to mobile devices, and get spectrum to train at both home bases and overseas locations that have similarly harmonized allocations. It is difficult to use current 4G LTE systems because, while the systems are available, the spectrum for U.S. systems was auctioned to telecom service providers for their commercial use. The future developments in the 3.5 GHz band may provide access to civilian technology with the spectrum to use it.

Unlicensed National Information Infrastructure devices provide short-range, high-speed unlicensed wireless connections in the 5 GHz band for, among other applications, Wi-Fi-enabled radio local area networks, cordless telephones, and fixed outdoor broadband transceivers used by wireless internet service providers. Unlicensed wireless broadband systems have become critical complements to licensed commercial mobile networks and to fixed wireline networks. For example, smart phones, tablets, net-books and laptops typically have inexpensive Wi-Fi capabilities that enable high-speed broadband connectivity in a wide array of locations.

Part 15 of the Federal Communications Commission's rules permits the operation of radio frequency devices without issuing individual licenses to operators of these devices. The Commission's Part 15 rules are designed to ensure that there is a low probability that these devices will cause harmful interference to other users of the same or adjacent spectrum.

Typically, unlicensed devices operate at very low power over relatively short distances, and often employ various techniques, such as dynamic spectrum access or listen-before-talk protocols, to reduce the interference risk to others as well as themselves. The primary operating condition for unlicensed devices is that the operator must accept whatever interference is received and must correct whatever interference it causes. Should harmful interference occur, the operator is required to immediately correct the interference problem or cease operations.

Beginning in 1997, the FCC continually took actions that would eventually make available 555 megahertz of spectrum in the 5 GHz band which is divided into several sections referred to as U-NII bands. The UNII-1 band 5.15-5.25 GHz was originally designated for indoor operations, UNII-2 and UNII-2A extended bands 5.25-5.35 GHz are for indoor and outdoor operations, and the UNII-3/ISM band 5.725-5.825 GHz is intended for outdoor bridge products and may be used for indoor WLANs as well. In a more recent attempt to satisfy the growing needs of businesses and consumers for fixed and mobile broadband communications, the FCC published it's First Report and Order on April 1, 2014 which slightly modified the rules for UNII-1 devices in the 5.15-5.25 GHz band; removing the indoor-only restriction and increasing the permitted power, thus increasing the utility of spectrum and accommodating the next generation of Wi-Fi technology.

In order to co-exist with military radar systems in the 5 GHz UNII-2A extended bands, radios must comply with two features that are part of the IEEE 802.11 specifications

(Continued on page 42)

(Continued from page 41)

which are Dynamic Frequency Selection and Transmitter Power Control. DFS dynamically instructs a transmitter to switch to another channel whenever a particular condition (such as the presence of a radar signal) is met. Prior to transmitting, a device's DFS mechanism monitors its available operating spectrum, listening for a radar signal. If a signal is detected, the channel associated with the radar signal will be vacated or flagged as unavailable for use by the transmitter. TPC is a feature of a digital microwave radio link that adjusts transmitter output power based on the varying signal level at the receiver. TPC allows the transmitter to operate at less than maximum power for most of the time; when fading conditions occur, transmit power can be increased as needed until the maximum is reached.

The Army, Navy, and Air Force operates Unmanned Aviation Systems in the 5 GHz frequency range for intelligence, surveillance, and reconnaissance; combat search and rescue; and real-time full-motion video for target development. The Department of Homeland Security also operates UASs in this band for drug interdiction and border surveillance operations. In addition, NASA also operates a limited number of systems in the 5.35-5.47 GHz band that are used for downlink transmissions of data to ground control receivers. The Department of Defense uses the 5.35-5.47 GHz band for a wide variety of ground based, shipborne, and airborne radars.

In 2012 Congress passed "Middle Class Tax Relief and Job Creation Act", in which section 6406(b)(1) required the NTIA in consultation with the Department of Defense and other impacted agencies, to conduct a study evaluating known and proposed spectrum-sharing technologies and the risk to federal users if the FCC allowed U-NII devices to operate in the 5350-5470 MHz and 5850-5925 MHz bands. Under current FCC regulations, U-NII devices are authorized to use 555 megahertz of spectrum in the 5150-5350 MHz and the 5470-5825 MHz bands subject to specific technical and operational restrictions to enable sharing with protected radar and satellite operations.

On February 20, 2013 by notice of NPRM, the FCC proposed to amend Part 15 of its rules governing the operation of Unlicensed National Information Infrastructure (U-NII) devices in the 5 GHz band. As stated, U-NII devices are unlicensed intentional radiators that operate in the frequency bands 5.15-5.35 GHz and 5.47-5.825 GHz, and which use wideband digital modulation techniques to provide a wide array of high data rate mobile and fixed communications for individuals, businesses, and institutions. The FCC wanted to revisit the original 1997 rules, and proposed to modify certain technical requirements for U-NII devices to ensure that these devices do not cause harmful interference and thus can continue to operate in the 5 GHz band and make broadband technologies available for consumers and businesses.

The FCC also sought comment on making available an additional 195 megahertz of spectrum in the 5.35-5.47 GHz and 5.85-5.925 GHz bands for U-NII use. This could increase the spectrum available to unlicensed devices in the 5 GHz band by approximately 35 percent and would represent a significant increase in the spectrum available for unlicensed devices across the overall radio spectrum.

The initiation of this proceeding satisfies the requirements of Section 6406 (a) of the "Middle Class Tax Relief and Job Creation Act of 2012" which required the Commission to begin a proceeding to modify part 15 of title 47, Code of Federal Regulations, to allow unlicensed U-NII devices to operate in the 5350-5470 MHz band.

The Commission believes that an increase in capacity gained from 195 MHz of additional spectrum, combined with the ease of deployment and operational flexibility provided by the U-NII rules would continue to foster the development of new and innovative unlicensed devices, and increase wireless broadband access and investment.

Dialog between the Wireless Communication Industry, Cable Company Representatives, the FCC, and the NTIA are still underway in trying to create a permanent solution for spectrum sharing in the 5 GHz band. Industry representatives along with the Department of Defense are working tirelessly to meet the President's intent to increase spectrum availability for future technological advancement by 2020.

Discussions are also still on-going internally between the wireless and cable industry in negotiating more efficient spectrum usage within the U-NII bands while extending current outdoor/ indoor wireless capabilities across the bands.

All federal and non-federal entities involved are diligently brainstorming to ensure the American people and Armed Forces abroad are getting the best possible telecommunication service available while satisfying the growing need for future wireless technological advancement in the United States.

Spectrum is a commodity that fuels America's dominance in innovative commercial systems that power mobility. This same spectrum is needed by the Department of Defense to conduct its mission of protecting our nation and providing our warfighters with the systems they need to succeed on the battlefield. While on the face, these two aims appear to be mutually exclusive, through cooperative spectrum sharing and continued innovation in sharing techniques, we can achieve both a vibrant economic future and a dominant, technologically strong military force.

CW5 Garth R. Hahn *is the senior Signal warrant officer at the I Corps, G-6 and former Fellow at the Federal Communications Commission. He began his military career in the satellite communications field in 1986. He has served tours in Belgium, Germany, Korea, Kosovo, Iraq and several stateside locations.*

CPT Bryant A. Wellman *is currently a Federal Communications Commission Fellow. He previously served at Fort Myer in the Army's Presidential Ceremonial Regiment "The Old Guard." He began his career in 2004 as a platoon leader in the 82nd Signal Battalion. Previous assignments also include the 82nd Airborne Division, 1st Space Battalion, and 53rd Signal Battalion.*

Join the Discussion

https://SIGKN.army.mil

Acronym QuickScan

4G – Fourth Generation
DFS – Dynamic Frequency Selection
FCC – Federal Communications Commission
FSS – Fixed Satellite Service
GAA – General Access Authorization
GHz – Gigahertz
IEEE – Institute of Electrical and Electronics Engineers
LTE – Long-Term Evolution
MHz – Megahertz
NPRM – Notice of Proposed Rulemaking and Order
NTIA – National Telecommunications and Information Administration
NASA – National Aeronautics and Space Administration
PA – Priority Access
PCAST – President's Council of Advisors on Science and Technology
RADAR – Radio Detection and Ranging
SAS – Spectrum Access System
TPC – Transmitter Power Control
UAS – Unmanned Aviation Systems
U-NII – Unlicensed National Information Infrastructure
Wi-Fi – Wireless Fidelity
WLANS – Wireless Local Area Networks

Starnet roadmap for the future network

By Claire Heininger

Capitalizing on feedback from Soldiers who took Capability Set 13 to Afghanistan and direction from senior leaders on advancing the network to support the next fight, the Army has developed a modernization roadmap that pushes toward an intuitive, dynamic and robust tactical network for Force 2025.

With some of the improvements already underway, the roadmap includes three phases that act as building blocks: Network 2.0 (Fiscal Years 2014-16), Simplified Tactical Army Reliable Network (STARNet, FY16-20), and the Network After Next (NAN, 2020 and beyond). The plan centers on making the network more versatile to support an agile, expeditionary force, as well as making communications systems easier for Soldiers to operate with less training and field support.

"The Chief of Staff of the Army has made it very clear that the network is a key enabler to getting the Army where it needs to go, which is essentially a leaner, more versatile force that has the ability to adjust based on mission, based on region, based on lots of different factors," said BG Daniel P. Hughes, program executive officer for Command, Control, Communications-Tactical. "We're looking to develop adaptive solutions that can meet these challenges, and to replace the complexity of the current network with complete simplicity."

The Current Network in Theater

Over the past two years, the Army fielded four of the final brigade combat teams bound for Afghanistan with Capability Set 13, an integrated network package that brought dramatic changes from previous communications equipment. CS 13 introduces mobile satellite and terrestrial communications that connect all echelons of the BCT with voice and data, allowing commanders and Soldiers to stay situationally aware at all times, even when far away from the command post. It extends the high-capacity Warfighter Information Network-Tactical Increment 2 network "pipe" to the company level, and brings the dismounted Soldier into the network with data radios and smartphone-like Nett Warrior devices that allow troops to send messages, access mission-related applications and track one another's locations with Global Positioning System technology.

Three of those BCTs have since deployed to Afghanistan as security force assistance brigades, which operate with fewer Soldiers and in different configurations than a typical BCT, to help execute the U.S. advise-and-assist mission and retrograde operations. While unit leaders say CS 13 has supported the SFABs in numerous expected and unexpected ways, they have also provided detailed and constructive feedback to the Army on how to improve the equipment for the future. [See CS-13 in combat: Adapting the network to the mission, page 28]

"It's new, and like anything new, it's going to take some time to work out the bugs and figure out how to make it more efficient," said MAJ Gary Pickens, 4th BCT, 10th Mountain Division (Light Infantry) S6, or 4/10, which concluded its deployment in March.

"Is it a home run right out of the gate? No, but it's a great step in the right direction."

MAJ Pickens said his unit gained the most value from two aspects of CS 13: networked key leader vehicles that eased the transition between command post and

mounted operations, and greater accountability of dispersed, dismounted troops. The vehicles integrated with WIN-T Increment 2 allowed key leaders to maintain access to mission command information and stay in constant contact with the rest of the brigade while far away from their tactical operations centers.

"On an expeditionary advising mission, you're going to gather a lot of data points," Pickens said. "You can call over a radio and dictate that stuff to a person at the other end, or keep notes in a notebook and do it when you get back to the base – so why not type it on the mission itself?"

At lower echelons, the Rifleman Radios and Android-based Nett Warrior devices that provided digital communications and Position Location Information for dismounted Soldiers served as a force protection measure that helped 4/10 cover more ground with fewer troops.

"We had these security and advisory teams going to pretty dangerous places where there had been a history of attacks against coalition forces," MAJ Pickens said. "Using the end user device, very quickly a leader is able to look at a map with his Soldiers arrayed on that map and understand with confidence what the situation is."

Challenges and Adaptable Solutions

That new "digital guardian angel" capability provided by the data radios, however, also introduced new complexities. Unlike traditional FM radios, the CS 13 Lower Tactical Internet requires a deliberate pre-planning effort to configure the Soldier Radio Waveform, and is difficult to adjust to account for unit task reorganization, a common occurrence for SFABs. The 4/10 S6 shop developed a temporary solution that pre-built SRW networks to their maximum size and assigned numbered presets for each platoon, which allowed operators more flexibility to switch networks as the mission required. But that workaround also had limitations, MAJ Pickens said.

Responding to this concern, the Army is now accelerating changes to simplify the network adjustments required to support UTR. For example, the On Demand Information Network app – developed in six months using an Android-based, open architecture – takes a step in the right direction, providing the ability to dynamically reconfigure software defined radios to support mission changes without ever having a Soldier touch a radio. As part of STARNet, the Army is developing a plug and play architecture that will allow seamless, automatic, over the air network reconfiguration associated with force structure changes through a user-friendly graphical interface and automated execution process.

"The Soldier will do a drag-and-drop on the screen," said Jennifer Zbozny, chief engineer for PEO C3T. "A lot will be going on beyond the scenes, but from the user perspective, he should just be able to say, 'I want to move my company over here.'"

Another challenge users encountered with CS 13 was more straightforward: much of the network equipment was integrated and delivered on family of medium tactical vehicles and mine resistant ambush protected all terrain vehicles, to meet force protection requirements for the Afghan theater. However, the SFAB mission often called for air movement rather than ground transportation, leading units to devise their own innovative ways to get CS 13 where they needed to go. [See CS-13 in combat: Adapting the network to the mission, page 28].

Similar feedback regarding vehicle platforms was provided by the 101st Airborne Division (Air Assault) and 82nd Airborne Division, whose BCTs have

(Continued on page 46)

(Continued from page 45)

also received CS 13 or the follow-on CS 14.

"We cannot sling an MRAP, and it's a challenge for us because of that," said CPT Alexander Marotta, deputy S6 for the 3rd BCT, 101st Airborne, which is training with CS 13. "That being said, it doesn't take away our ability to use these systems to enhance our mission command. There are a lot of positive things that are coming out that we can still utilize without air assaulting the large pieces of equipment."

The Army has begun to deliver CS 14 equipment on different platforms, including high mobility multipurpose wheeled vehicles and Strykers, to fit unit requirements, and is working to make the equipment more scalable and tailorable.

"There is no single cookie cutter solution that can fit all forseeable missions, but having adaptable components, and more importantly adaptable people that offer options, is invaluable," said MAJ Graham Wood, S6 for the 3rd BCT, 10th Mountain Division, which is currently deployed with CS 13.

MAJ Pickens agreed, describing the network as an adjustable collection of capabilities that add to a unit's overall arsenal.

"A professional mechanic is going to have a toolbox with 5,000 different tools in it – some he's going to use all the time, some he's only going to use once a year," MAJ Pickens said. "CS 13 gives more tools to a commander to have in their kit, and the mission set, the units going into it and the commander's vision to accomplish that mission is what's going to drive which tools are employed."

Simplify, Simplify

The most universal lesson-learned from CS 13 is the need to simplify tactical communications systems so they pass the "iPhone test": easy for Soldiers to operate with minimal training or intervention by civilian field support representatives. Simplicity is the common element that stretches across the different focus areas of the network modernization roadmap, which include mission command, upper and lower tactical internet transport, cyber, network operations tools, and physical enablers such as power requirements and command post footprint.

Network 2.0, the first phase of the plan, is already underway. It focuses on providing a converged and enhanced network baseline for the Army to build upon for future capability sets, by continuing to transition stand-alone mission command systems into integrated, web-based applications and by simplifying and converging NetOps tools for the S6 and G6.

Network 2.0 also delivers critical upgrades for the WIN-T Increment 2 Key Leader Vehicles, including major reductions in startup and shutdown times, a simplified graphical interface and improved troubleshooting tools. The improvements are being validated and tested this summer and fall in preparation for fielding to CS units.

Those changes will make the vehicles more accessible for the general-purpose user and increase their utility on the battlefield, Marotta said.

"We're going to see the Soldiers want to use it," he said. "It's a great new capability and I can't wait for it to go through some of its growing pains."

STARNet, the mid-term phase that concludes in 2020, will begin to inject next-generation technologies into the network baseline to deliver a more seamless information-sharing environment, allowing users to connect and collaborate across operational phases, echelons, regions and partners. Using standardized maps, messaging and icons, STARNet will provide a unified, familiar experience

across the command post, mounted and dismounted environments – similar to what a user would have with multiple personal devices that all run an Apple, Google or Windows operating system. STARNet will also lighten network systems' energy burden and leverage wireless technology for quicker setup and teardown of command posts.

"Consolidating hardware, reducing power requirements and using Wi-Fi and 4G/LTE will help unclutter the TOC, leading to faster setup time to support dynamic operations," Zbozny said.

NAN defines the objective tactical network capabilities and leap-ahead technologies to support Force 2025. NAN will enhance tactical cyber operations, add dynamic spectrum access solutions for greater bandwidth and introduce digital assistants that provide needed information, analyses and recommendations on a complex battlefield.

After defining the detailed technology goals for each phase of the roadmap, PEO C3T is now collaborating with the Army G-3/5/7, Chief Information Officer/G-6 and G-8; Training and Doctrine Command Centers of Excellence; Network Enterprise Technology Command; Science and Technology Community; industry partners and others to align the requirements and funding to continue executing the plan.

"Our goal and our imperative to support Force 2025 is to provide commanders and Soldiers with the information and connections they need to execute decisive actions anytime, anywhere and on any device," BG Hughes said. "The feedback and innovation from CS units has been invaluable as we simplify and shape the network for those who will follow in their footsteps."

Claire Heininger *is a staff writer for Symbolic Systems, Inc., supporting the U.S. Army Program Executive Office for Control and Communications-Tactical. She is a graduate of the University of Notre Dame, a former reporter for the Star-Ledger (New Jersey's largest newspaper), and has covered Army network technologies since 2010.*

ACRONYM QuickScan

4/10 – 4th Brigade Combat Team, 10th Mountain Division
BCT – Brigade Combat Team
CS – Capability Set
FMTV - Family of Medium Tactical Vehicles
HMMWV - High Mobility Multipurpose Wheeled Vehicles
MATV - Mine Resistant Ambush Protected (MRAP) All Terrain Vehicles
NAN – Network After Next
ODIN – On Demand Information
PEO C3T – Program Executive Office Command, Control, Communications-Tactical
SFAB - Security Force Assistance Brigade
STARNet - Simplified Tactical Army Reliable Network
SRW – Soldier Radio Waveform
TOC – Tactical Operations Center
UTR – Unit Task Reorganization
WIN-T – Warfighter Information Network-Tactical

New satellite terminal program increases network capacity and reach

By Amy Walker

As the Army's current and future operational landscape continues to change, new suitcase-sized satellite equipment will extend the service's tactical communications network backbone, Warfighter Information Network-Tactical, to the tip of the spear, while providing up to 16 times the throughput of currently fielded capability.

"Some battlefields require Soldiers to be close together like in conventional wars, but other battlefields, such as low intensity conflicts or counterinsurgency operations, require units to be well dispersed," said LTC Joel Babbitt, product manager for WIN-T Increment 1, which currently manages the new program.

"This new equipment enables the Army to provide high volumes of data at high speeds to companies and teams that are dispersed at the farthest tactical edge."

The Transportable Tactical Command Communications program will provide satellite dishes that deploy in transit cases the size of carry-on luggage to support small detachments and teams, plus larger transportable satellite dishes that can be carried in the back of a truck to support company-sized elements. This advanced technology will enable Soldiers to connect to the WIN-T network even in remote locations void of network infrastructure.

In early May, the Army Acquisition Executive signed the Material Development Decision for the T2C2 package, which establishes T2C2 as a formal Army POR. A Milestone C decision is expected in May 2015. The Initial Operational Test and Evaluation is currently scheduled for the Network Integration Evaluation 16.2, followed by a full rate production decision and fielding to units.

"T2C2 directly addresses the Army's current priorities of becoming a more expeditionary, scalable and capable force," LTC Babbitt said. "Additionally, by providing continued higher capacity network communications to the most remote locations, we're enabling much more robust situational awareness and mission command capabilities for smaller units dispersed throughout a broader battlespace."

There are two versions of T2C2 – a light and a heavy version. The man-portable T2C2 "Lite" can be set up and on the air in less than 10 minutes. It is transported in two transit cases the size of carry-on luggage. As part of the WIN-T network, T2C2 provides satellite capability to small detachments and dismounted teams operating in remote locations without network infrastructure, enabling them to securely relay information and increasing situational awareness for the entire operation. It provides high data throughput to support large data files like imagery, video or biometrics information.

(U.S. Army photo)

Transportable Tactical Command Communications (T2C2) Lite is similar to the Army's legacy Global Rapid Response Information Package (GRRIP), shown here, but utilizes U.S. military satellites and provides significantly increased throughput.

Although the final prototype or vendor of T2C2 has not yet been determined, one potential version of the T2C2 Lite was demonstrated at NIE 14.2 in May at Fort Bliss, Texas. The 2nd Battalion, 8th Marine Regiment used the prototype

(U.S. Army photo)

As part of the Warfighter Information Network-Tactical communications network, Transportable Tactical Command Communications Lite provides satellite capability to small detachments and teams operating in remote locations without network infrastructure, enabling them to securely relay information, increasing the situational awareness for the entire operation.

to extend communications from the WIN-T backbone out to small teams. Additionally, a number of Army units are already utilizing potential T2C2 Heavy solutions in theater via fielded operational needs statements.

T2C2 Lite is similar to the Army's legacy Global Rapid Response Information Package, a non-POR, suitcase-sized ground satellite capability, which leverages commercial satellite technology only. Due to the nature of their missions, certain detachments and small teams may require a great deal of bandwidth to run more advanced applications. By basing T2C2 on military Ka and X band the program enables access to the Department of Defense-owned advanced Wideband Global SATCOM constellation, T2C2 Lite provides significantly higher throughput over legacy capability. It jumps from kilobits per second to megabits per second, providing up to 16 times more throughput needed to run advanced applications.

"The Army has used expensive commercial bandwidth almost exclusively for more than almost 13 years now," said Tim Fitz Maurice, T2C2 lead for PdM WIN-T Increment 1. "These dishes plus the Department of Defense-owned WGS satellite constellation equals a significant reduction in cost, both from top level and unit level, by avoiding reliance on commercial SATCOM."

While T2C2 Lite provides SATCOM to early entry teams and will be a pooled resource at brigade combat teams, the larger T2C2 Heavy provides a high bandwidth tactical network extension for small companies and small forward operating bases operating beyond-line-of-sight from their higher headquarters. The heavy version will enable small at-the-halt command posts and maneuver company-sized elements to exchange critical situational awareness over the WIN-T network. The bigger dish size compared to the Lite version also means more throughput from the same amount of satellite bandwidth.

"Instead of companies only having radio communications, T2C2 heavy extends the WIN-T network down to a company

(Continued on page 50)

(U.S. Army photo)

Transportable Tactical Command Communications enables companies operating in remote locations without any network infrastructure to securely relay situational awareness from anywhere on the planet.

(Continued from page 49)

FOB," Fitz Maurice said. "So a company in a remote outpost can have Command Post of the Future, mission command applications, email and other network capabilities they need to better support a successful mission."

Army leaders are looking to use legacy Secure Internet Protocol Router/Non-secure Internet Protocol Router Access Point ground satellite terminals and GRRIPs as a bridging capability for T2C2 Heavy and Lite respectively, until the final T2C2 capability is eventually fielded. The basis of issue plan for the SNAP and GRRIP bridging capability is very closely aligned with that for T2C2, so as T2C2 eventually begins fielding, PM WIN-T will just replace those legacy systems with the new, more advanced capability.

By providing continued higher capacity network communications to the most remote locations, the Army is enabling robust situational awareness and mission command capabilities at tactical edge through all phases of operations.

"No matter where they are called to deploy, Soldiers using T2C2 will be able to access and send the information they need," LTCV Babbitt said. "It provides range extension to areas that were not previously linked in to the tactical network backbone, reaching out and extending that network coverage like never before."

(U.S. Army photo by Amy Walker)

Transportable Tactical Command Communications Heavy will provide small company sized units with satellite network communications capabilities similar to the Army's legacy high-bandwidth Secure Internet Protocol Router /Non-secure Internet Protocol Router Access Point ground satellite terminals, but with advanced capabilities that include military satellite and secure Colorless Core capability. The SNAP shown here was part of the Network Integration Evaluation 13.1 at White Sands Missile Range, N.M. and Fort Bliss, Texas.

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

Acronym QuickScan

FOB – Forward Operating Base
GRRIP – Global Rapid Response Information Package
NIE – Network Integration Evaluation
POR – Program of Record
SATCOM – Satellite Communications
SNAP – Secure Internet Protocol Router/Non-secure Internet Protocol Router Access Point
T2C2 – Transportable Tactical Command Communications
WGS – Wideband Global SATCOM
WIN-T – Warfighter Information Network-Tactical

Enterprise security system deployment

By MAJ Scott A. Salmon

Many people cringe when they hear the phrase, "information assurance compliance."

It seems the term is synonymous with "no you can't" or it's going to be a difficult process that has to be approved at the senior level to do something that seems so simple on your home computer system.

Effective security is seldom convenient or easy. If it were easy it wouldn't be worth doing. I'm sure the enemy would like for it to be both convenient and easy.

Information security requirements have always existed, but only brought to the forefront of importance and leader focus in recent years due to major incidents involving national security with emerging technologies, vulnerabilities and impacts to unit mission.

U.S. Army Central Command in coordination with the 335th Signal Command (Theater) (Provisional) engaged the Defense Information Systems Agency for a comprehensive security compliance tool that has the ability to automate and report the security posture of a networks key components.

The requirement for a tool that will consolidate and supplement existing IA tool data collections to increase situational awareness and enhance the security posture to meet IA compliance for certification and accreditation, vulnerability management and asset tracking in a user friendly dashboard view. DISA responded to our request with the identification of a tool they've been using for years to meet their compliance requirements. ESPS is a comprehensive security compliance tool created at DISA Defense Enterprise Computer Center in Montgomery, Ala. This tool has enhanced capabilities that supplement other IA tools and provides situational awareness of the security posture of all servers, databases, and systems for Security Technical Implementation Guide, Information Assurance Vulnerability Assessment, Security Content Automation Protocol compliance checker and Vulnerability Management System file generation to upload across multiple operating system platforms. The partnership with DISA in piloting this system will provide a snapshot for leaders to consider making this tool available to all of DoD as an enterprise service offering.

Enterprise Security Posture System provides a Graphical User Interface to view compliance status on a dashboard for servers, databases, and workstations. This tool was created internally at DISA DECC Montgomery to meet their IA compliance requirements in an automated, cost effective manner. ESPS has enhanced capabilities that supplement existing IA tools with the scalability to support future tools. ESPS was developed to provide automation and detection that no other tool provides. Other tools such as HBSS Policy auditor, Space and Naval Warfare Systems Command SCAP Compliance Checker, 3.0 and the STIG Viewer do not provide the complete review of all applicable STIGs, IAVMs, policies and SCAP checks that is provided by ESPS. For example, the SPAWAR SCC tool had 356 of the 614 checks that are in VMS for the windows operating system.

In addition, SCC doesn't cover any of the additional targets for the Windows OS like McAfee, Internet Information Services, and Domain Name Services. Other tools provide a portion of these checks, but only ESPS provides all necessary checks in an automated fashion and reports that are easily understood by information assurance security personnel. This tool utilizes Unix and Windows scripts that are developed to encompass and supplement FSO toolkits (Gold Disk, SRR, Winbatch). One of our newest improvements

(Continued on page 52)

(Continued from page 51)

in ESPS is the incorporation of Retina and Assured Compliance Assessment Solution Nessus scan data. This capability further improves the visibility of the complete security posture of an asset. Once incorporating the toolkit, which is essentially an agent loaded on servers and workstations, it will check in with the master database and schedule scans and upload of automated data collections that are organized and available for report generation. If the existing reports do not meet the individualized needs of a unit, a request for change can be submitted for customized reports. Initial piloting of ESPS is complete at the Main Command Post, this system will be further deployed throughout the South West Asia area of responsibility in coming months for integration into business processes and greatly assist with the IA security posture and certification and accreditation challenges in that environment.

Information security requirements will continue to exist as the enemy will continue to try and exploit information that they are not intended to have. If we can mitigate the occurrence of major incidents involving national security with technology, we have to keep up with emerging technologies available to our enemies to subvert vulnerabilities that impact mission readiness and the ability to command and control.

MAJ Scott A. Salmon
graduated from Central Missouri State University, with a Bachelor Degree in marketing. and was commissioned in 2001. He earned the Certified Information Security Manager certification in 2010 and has completed the Signal Captains Career Course. MAJ Salmon has served a variety of increasingly responsible Signal positions including platoon leader, battalion FA53 automation officer, battalion S6, USARCENT HQ support operations officer in charge of networks, systems and helpdesk, information assuarance program manager and information assurance manager.

ACRONYM QuickScan

ACAS - Assured Compliance Assessment Solution
DISA - Defense Information Systems Agency
DECC - DISA Defense Enterprise Computer Center
DNS - Domain Name Services
ESPS - Enterprise Security Posture System
GUI - Graphical User Interface
IA - Information Assurance
IAVA - Information Assurance Vulnerability Assessment
IIS - Internet Information Services
SCC - SCAP Compliance Checker
SCAP - Security Content Automation Protocol
STIG - Security Technical Implementation Guide
SWA - South West Asia
SPAWAR - Space and Naval Warfare Systems Command
USARCENT - U. S. Army Central Command
VMS - Vulnerability Management System

Operating an effective Afghanistan network

By COL Stephen Hager

The battle to improve our strategic network while engaged with on going combat operations is a difficult task.

While in Afghanistan for OEF, the Signal community provided the Commander with C5ISR capability, while drawing down the forces and the physical infrastructure to support the strategic communications network. Much of this is driven by the desire for a reduction in Force Manning Levels and lower operational costs. Simultaneously, we had to improve the network security and support the enterprise initiatives to achieve the cost savings DoD is projecting.

At the height of the surge, the Signal community proliferated the battle space with over 25 Technical Control Facilities. These data centers were the hub of the network with most data services residing in these locations. At the time, many were single threaded over a TACSAT or Multichannel Line of Sight connection.

Likewise, Network Operations Authorities were held at the local regional commands, providing decentralized NETOPS through out the Combined Joint Operation Area – Afghanistan. For the surge, this was the right approach. The expanding and every changing dynamics of the battle space required local NETOPS to be responsive to the regional commanders.

Over time, the physical infrastructure grew, with fiber, MLOS, and satellite providing connectivity to the main sites. By Feb 2013, most of the TCF's had two or three forms of connectivity—fiber being the preferred. This triple redundancy provided a very high level of up time to the Strategic network. Most outages were the result of power, HVAC issues, or improper change management.

Improved Infrastructure and Target Network Architecture

During the drawdown, the Signal community was challenged to reduce FML. Having the Afghans take the lead for security and force protection and retrograde operations were the key efforts. A target network architecture was developed and by June 2013, execution was well underway.

By the election in April 2014, we had reduced the number of TCF's to a dozen. Sites that did not have a local TCF pulled services remotely and had small data stacks for local requirements (such as call managers and shared drives). These remote sites did not have large subscriber counts and were essentially "long local" to one of the enduring hub sites. Additionally, the remote site would have double or triple redundancy for transport (fiber, MLOS, Satellite). The enduring hub sites would have two TCF's, which provided application level redundancy.

Simultaneously, while reducing the number of TCF's, we also executed a number of strategic projects to increase redundancy at all layers. Starting with the enduring TCF's and ADN's, we installed redundant diversified fiber—ensuring physical path redundancy. Additionally, we installed Virtual Switching System, ensuring uptime of the core switches at the network layer. We also installed High Availability Data Groups for Exchange and SharePoint providing application level redundancy while also significantly reducing the number of servers.

The virtualization of servers in the TCF's allowed for a reduction in physical servers and allowed us to provide more compute power per rack.

This effort allowed us to consolidate services at central points and helped with the overall reduction of TCF's. While this is a natural improvement in technological advancement, it helped immensely by increasing the subscriber count a single TCF can support. The downside was that there was an increase in power and HVAC for the individual TCF that housed the consolidation of services.

Additionally, introducing more military

(Continued on page 54)

(Continued from page 53)

spectrum capable systems into the network reduced satellite transport costs. The commercial use of satellite airtime was very expensive, but at the time of the surge was the proper way to expand our transport footprint. Over time, by replacing some of the Ku with Ka band terminals, we were able to lower operational costs and increase reliability and survivability for satellite transport.

There are many opportunities to reduce cost while providing similar IT services—but we must be aware of the technology trap -- of throwing money at the latest technical solution which becomes outdated before it can be implemented and deployed -- then chasing the latest technology trend. All large enterprise organizations face this challenge, and the Army is no different.

MPLS (Multi-Protocol Label Switching) is a mature technology that the DoD is starting to embrace. It basically is a way to classify your traffic upon ingress into a network, prepend a special tag and switch it through the core network until it reaches the egress device and the tag is stripped off. This essentially, encapsulates your data traffic within the tagged frame. The improvement to typical IP- based routing, is that you can have pre-determined paths with Quality of Service as well as automatic failover should a physical path become unavailable.

A major effort by the Signal community was to migrate the Air Force users at Kandahar Air Field off of the Air Force network onto the USFOR-A network. There were many issues in dealing with a common desktop image, running parallel networks simultaneously while keeping Air Force Mission Essential Functions operational while physically migrating the users. And because of the hard work and determination of those involved with the migration the effort was a complete success. It should be seen as a major effort towards the Joint Information Environment where multiple services can work together to provide a communication solution for the war fighter.

Potential Improvements

In retrospect, Transport as a service would have solved the issues of migrating the Air Force users at Kandahar onto the USFOR-A network (an Army network). If we expanded MPLS L3VPNs to the desktop we would simply map the Air Force users to an Air Force L3VPN. However, providing a L3VPN to the desktop is not feasible, but we could have developed a solution that is almost as good by combining Layer 3 MPLS VPN's and L2 Tagged VLANs.

Our current model is to have TCF's (data centers) interconnected into an MPLS cloud. The Label Edge Router that does the packet classification on the ingress and conversely strips the label at the egress is located at the TCF.

Inbound traffic comes from the desktop to the EUB switch, into an ADN, then the TCF. At the TCF, the packet gets classified with a MPLS label. It then enters the MPLS cloud and follows the Label Switch Path to the distant end—probably another TCF. From the distant end TCF, the traffic is sent to the Area Distribution Node, then onto the End User Building.

If you tried to push MPLS out to the edge EUB, it would not scale. The TCF's, ADNs, and EUB's would all have to be in the MPLS cloud. The LER would reside at the EUB and that would be very hard to manage.

However, you can use L2 VLAN's out to the EUB, then untag the L2 packet as it goes to the desktop. Thus you can have a VLAN for the Air Force that is tagged at ingress port on the EUB, goes through an L2 Trunk port to the ADN and is then mapped to an L3VPN at the TCF.

We currently have multiple L3VPN's we run in our Enterprise Black core network (eBCN). There are less than 4,095—which is the total number of VLANs an L2 switch can support. So mapping them would not be too difficult. The protocol to take any L2 access port and assign an ingress VLAN id is MVRP (Multiple VLAN Registration Protocol). All the uplinks from the EUB to the ADN now become Trunk ports (carrying L2 tagged VLAN packets).

The need is to configure the EUB ingress port that goes

to the desktop to have the appropriate L2 VLAN ID that will be mapped to the correct L3VPN. If the entire building were to be Air Force users, we can manually map that entire EUB switch to have the correct L2 VLAN ID.

However, it would be clever to dynamically assign the L2 VLAN ID based on the user's login credentials. Currently, using 802.1x is used for port security, and it has dramatically reduced the number of cross-domain violations. It essentially blocks all traffic from a network device until that device is registered as "authorized" to be on the network. It then unblocks the port and allows normal data traffic to flow through that port.

At this point, theoretically, MVRP would kick in and, based on the user's credentials, set the access port to the appropriate VLAN ID and propagate that VLAN ID to all other L2 switches (such as the aggregation switch at the ADN). The mapping of the users credentials to the L2 VLAN ID would be an MRP (Multiple Registration Protocol) application that talks to the switches.

The end result could be that someone (Army, Air Force, Marine, Navy) uses a CAC or SIPR token card to login at any machine. That machine, then dynamically gets the appropriate VLAN assigned at the access switch (EUB), is cross connected to the appropriate L3VPN at the TCF and pulls application services from the appropriate military branch. This moves us closer to the JIE construct, allowing us to design a network that is agnostic to the specific requirements of the service. It provides a reliable transport network that maps the end user to the appropriate service component that specializes in the application delivery that the individual user needs.

The strategic network in Afghanistan is probably the most redundant and reliable communication network in a modern combat zone. Because of the great team effort of the Army, Air Force, Navy, Marines, DoD civilians, and contractor work force, the Department of Defense Information Network allowed for real time operations from around the world. Like all military communication professionals, our goal is to improve the concepts and lessons learned from our current engagement to be better prepared for our next operation. By considering how to dynamically provision a virtual circuit (via MPLS L3VPN's and L2 VLAN ID's) to an end user based on login credentials, we are expanding the correct user capability to the edge. This reduces costs and improves security—both key tenets as we move towards JIE.

COL Stephen Hager *most recently served as the 335th Signal Command (Theater) (Provisional) deputy commander in Afghanistan. He has commanded at the brigade, battalion and company level. He has a BS in Mathematics, MS in Computer Science and a Masters of Strategic Studies. He has over 20 years designing high-speed data networking equipment in Silicon Valley.*

Acronym QuickScan

ADN – Area Distribution Node
C5ISR – Command, Control, Communications, Computers, Combat Systems, Intelligence, Surveillance, and Reconnaissance
CAC – Common Access Card
CJOA-A – Combined Joint Operation Area – Afghanistan
EUB – End User Building
FML – Force Manning Level
HVAC – Heating Ventilation Air Conditioning
JIE – Joint Information Environment
L2 – Layer 2
L2 VLAN – Layer 2 Virtual LAN (0-4095)
L3VPN – Layer 3 Virtual Private Network
LSP – Label Switch Path
LER – Label Edge Router
MLOS – Multichannel Line of Sight
MPLS – Multi Protocol Label Switching
MRP – Multiple Registration Protocol
MVRP – Multiple VLAN Registration Protocol
NETOPS – Network Operations
OEF – Operation Enduring Freedom
TACSAT – Tactical Satellite
TCF – Technical Control Facility
VSS – Virtual Switching System
USFOR-A – U. S. Forces - Afghanistan

Keeping Warfighters connected during Phase 4 Operations

Signal retrograde from Afghanistan

By COL Linda C. Jantzen and LTC Jeffrey J. Thompson

U.S. Forces-Afghanistan is in the midst of a massive retrograde and redeployment effort as combat operations in Afghanistan are transitioned from the United States and North Atlantic Treaty Organization forces to Afghan security forces.

As forward operating bases close or are transferred to Afghan or other government agency control, the theater communications network infrastructure, which had at its peak expanded to 23 strategic technical control facilities along with hundreds of tactical extensions, has to be scaled back without interrupting critical network services to support the remaining mission.

With lessons learned from Iraq and recent experience de-commissioning and moving a modular technical control facility from Afghanistan to Kuwait, the 160th Signal Brigade and mission partners in Afghanistan began the planning process to successfully retrograde the network.

The term "retrograde in contact" is used to describe maneuver forces transitioning from combat operations to train, advise, and assist roles, even as the enemy continues to engage them on a regular basis.

From a network perspective, the term describes the Signal community's efforts to dismantle the infrastructure while ensuring communications remain live and accessible wherever required to continue supporting the maneuver plan. At the same time, high value information technology equipment has to be accounted for throughout the packing, shipping, receiving and storing process. People with the right skill sets have to be on hand to accomplish the many tasks needed to migrate services, de-commission and dismantle a modular technical control facility.

All of this activity is collectively called Signal Retrograde Operations. It requires input and cooperation between communications providers and integrators, IT engineers, battalion/brigade/regional command and corps Signal staff, property technicians, resource managers and contracting officer's representatives, transporters, customers, commanders and battlespace owners.

A review of lessons learned from Iraq in 2011 offered useful hints, but the situation in Iraq 2011 and Afghanistan today is different in many important ways.

In Iraq, unanticipated political events forced tens of thousands of U.S. personnel to leave the country in a short period of time, giving communications providers very little time to shut down gracefully. Compounding the problem was that there were multiple communications providers, including multiple tactical signal elements with user- owned servers and connectivity under the control of different units, and an expeditionary Signal battalion under the 160th Signal Brigade which was operating and maintaining the theater S-IRAQ network. Many users in Iraq did not know how their communications was provided, nor how or who to coordinate with for continued service throughout the retrograde.

USFOR-A started the planning process early, triggered by the President's announcement of a reduction in boots-on-the-ground to 34,000 by February 2014. III Corps led the effort upon its arrival in April 2013, bringing maneuver units and all functional task forces together to produce a retrograde operations order, "Operation DRUMBEAT."

Meanwhile, U.S. Central Command leaders authorized Army Central Command to establish the CENTCOM Material Readiness Element as the lead for retrograde logistics in Afghanistan.

Ultimately, the details of how to collapse

the network, de-commission and ship strategic signal assets like modular technical control facilities and Deployable KU-band Earth Terminals back to Kuwait were left up to the Signal community.

Early in 2013, the 335th Signal Command (Theater) (Provisional) convened a Tactical Communications Facility Closure planning session in Bagram. 335th Signal Command (T)(P) engineers had published a notional communications architecture based upon decisions made by CENTCOM and USFOR-A as to the geographic footprint, operational and sustainment forces, and other functions that would endure following Operation Enduring Freedom transition to Resolute Support by the end of 2014.

The Signal planning session brought together the Regional Command CJ6s (1st Infantry Division and 3rd Infantry Division at the time) along with CENTCOM, International Security Assistance Force-Afghanistan Joint Command and USFOR-A CJ6 and the 160th Signal Brigade's headquarters element in Afghanistan known as Task Force Signal.

Discussions at the TCF Closure session made it clear that a single focal point would be needed to continue to plan, coordinate, execute, track and provide a common operational picture of network retrograde operations. Because no amount of planning could prevent the inevitable changes and conflicting information from various headquarters, staffs, mayors, battle space owners, contractors, etc, there had to be one place to receive the information coming from all levels at higher headquarters down to the lieutenant or sergeant first class on the ground at the TCF, de-conflict it, garner decisions, issue orders and inform the appropriate stakeholders. That "one stop shop" was the Signal Retrograde Operations Center-Afghanistan, stood up at and staffed by Task Force Signal headquarters in Bagram.

Having been briefed on the Signal retrograde concept for Afghanistan, MG Steve Smith, then commanding general of 335th SC(T)(P), asked COL Linda Jantzen, 160th Signal Brigade and Task Force Signal Commander, "who is your BRAC coordinator?" The term "BRAC," for base realignment and closure, was a vivid analogy to the Congressionally mandated process of closing and transferring DoD bases, which last occurred in 2005-6. The choice was clear for what soon would be known as the SROC-A Director.

As the former Joint Network Control Center-Afghanistan Director, LTC Jeffrey Thompson had expertise in all of the technical and logistical lines of effort that the SROC-A would be managing. His task was to centralize control of the signal retrograde process, create templates and Tactics, Techniques, and Procedures, apply lessons learned to make the process effective, efficient, and repeatable as personnel constantly flowed in and out of theater. SROC-A established a future operations capability that freed up the JNCC-A to focus on operations and maintenance and optimization of the remaining network.

The specific lines of effort established for the SROC-A follow:

Battle Tracking

This LoE provides asset visibility, identifies decision points and priorities for shared resources. Maintains master battle rhythm calendar to deconflict the various coordination meetings and working group sessions.

Network Transition

This LoE ensures continuity of network capabilities for customers remaining on a FOB after the TCF is shut down, migration of services to enduring hubs, and an orderly transition to the objective Resolute Support architecture. Uses on-location joint site surveys to identify user requirements and the right contingency package for sites in which a TCF will have to be de-commissioned and removed. This LoE ensures maximum use of existing infrastructure while phasing out excess capacity for use elsewhere.

(Continued on page 58)

(Continued from page 57)

Property Accountability

This process ensures all unit and contract property is accounted for and properly transferred from the shipper to the receiver, whether the asset goes into storage in Kuwait or is re-purposed to another unit or elsewhere in the network. This is a complex process given all the property types TF Signal has to deal with, from organizational (organic or deployed unit property), to theater provided equipment to government furnished equipment to "found on installation" equipment. All equipment had to first be placed on the correct property book based upon its final disposition.

Shipping

This involves multiple personnel, from the direct signal support team on the ground to the contractors responsible for operating and maintaining the facility, and still other contractors who have the ability to dismantle a modular TCF. This line of effort is also responsible for container management, blocking and bracing material, and transportation movement requests.

Logistics and Sustainment

This LoE ensures life support is in place throughout the de-commissioning and migration timeline. It also coordinates for force protection, class I support, material handling equipment, fuel and power support, etc. as necessary. Coordination with mayors/garrison staff is critical to ensure support for each of the other LoEs is available.

Contract Management

This LoE has oversight of information technology personnel and services contracts managed by Task Force Signal. Each contract has different rules of engagement. For example, all strategic TCFs are operated and maintained by the 160th Signal Brigade's contract with Operations, Maintenance and Defense of Army Communications in Southwest Asia and Central Asia. When a TCF comes out of system, the slots for personnel who operate and maintain that facility must be cut from the contract. Smaller sites are supported by Soldier teams or another contract which allows the operations and maintenance personnel to be re-allocated to another site or mission. Leased transmission services such as Microwave Line of Sight, fiber circuits, and satellite links must be terminated in a timely manner to avoid additional cost to the government.

Key to the success of signal retrograde operations in Afghanistan thus far have been several factors that were lacking or non-existent during the Iraq retrograde, the most salient one being time to plan and prepare. But other factors are perhaps even more important to understand, because they may influence how we build, operate and maintain operational base communications networks in the future:

Robust Transmission Pipes

Instead of each site hosting its own data and services, users can pull from neighboring sites with little latency due to the large bandwidth of fiber and MLoS between sites. The user experience is critical on an operational network. Remote hosting of network services such as Dynamic Host Configuration Protocol, Domain Name System, directory services, etc., provides the foundation to begin migration of application services. Transparency to the user is created by maintaining network services without changing or reconfiguring user desktop settings. Robust transmission paths enable greater bandwidth throughput, alternate pathways (e.g. fiber, MLoS, and SATCOM), and traffic shaping to give precedent to higher priority traffic. Migration of remote network services is phased over time to ensure dependable delivery before reaching end of mission on local services. Phasing of network service begins with a small pilot group from the Signal Community. After testing and validation from the pilot group is completed the remaining user community on the local Forward Operating Base is usually migrated overnight. Local networks services remains

running in a warm status during migration but the service are provided off site by a neighboring enduring location.

The applications (i.e. email, SharePoint) that are dependent on a solid network can now be migrated off site. Migration of applications is determined by user precedent (i.e. general officers or very important personnel), alphabetic grouping of common user group and finally the enclave to be migrated. The larger user community migrates first in alphabetical order to control any misconfiguration impact at a manageable level.

The VIP group is migrated last after all the "bugs" have been worked through and mitigated. Migration of applications off site creates an enterprise service environment to centralize services and reduce hardware and personnel at local TCFs. The operational environment drives all scheduled network changes.

The operational environment will also dictate which network enclave (e.g. Non-secure Internet Protocol Routing, Secure Internet Protocol Routing or CENTRIXS-ISAF) is migrated first or last.

Overall, the robust and redundant paths in Afghanistan enable enterprise service delivery and remote network management that will allow a huge reduction in the Signal footprint.

Centralize, Standardize and Optimize

Task Force Signal is the sole Signal command and control element for all echelon above Division signal units supporting USFOR-A, combining resources provided by USFOR-A, ARCENT, and Network Enterprise Technology Command under one Signal Brigade. This consolidation of network O&M allows for sharing of scarce resources and flexibility to shift those resources to where they are needed. It also ensures unity of effort and a single point of contact for the majority if not all communication issues and actions within Afghanistan. A single point of contact to coordinate large retrograde efforts with multiple lines of effort is critical on an operational network. The reduction of personnel manning levels is a forcing function to streamline command and control across all warfighting functions. Communications support under one command structure creates the conditions for equitable and informed decision resource disposition. Sharing of resources enables fewer "have-nots" with regards to communications capabilities. This decreases or eliminates the "have-nots" with regards to communications capabilities, and the ability to cover gaps in service created by departing units, end of contract period of performance, etc. Simultaneously, the more the network can be standardized and optimized for remote management, the smaller the footprint required to maintain it. As Task Force Signal headquarters in 2012, the 11th Signal Brigade created the Network Transition and Optimization Plan to do just that. It is a process whereby Signal planners and engineers come up with network optimizing objectives, tasks are assigned through the orders process, and progress is reviewed through regular NTOP sessions hosted by the Joint Network Control Center-Afghanistan.

One Network versus Two

The afghan.swa network is a child domain of the SWA theater network, not a completely separate domain like the S-IRAQ network. With the departure of the JNCC-Iraq, the SWA Cyber Center and the 54th Signal Bn had to quickly absorb responsibility for an entirely separate network. S-IRAQ served its customers well, so long as there was a robust NetOps and O&M capability dedicated to running it. But it could not easily be scaled down or gracefully handed off to a separate provider. The top level architecture stack for S-IRAQ had to be physically relocated to Kuwait and turned over to the 54th Signal Bn. In Afghanistan, customers can be seamlessly migrated from a strategic node

(Continued on page 60)

(Continued from page 59)

to a tactical extension of the SWA network, and NetOps functions continue uninterrupted even as the Regional Network Control Centers and eventually the JNCC collapse into one Regional Network Operations and Security Center operated by the 25th Signal Bn. Already strong NetOps working relationship with the Southwest Asia Cyber Center under the 11th Theater Tactical Signal Battalion, it grew tighter with both SWACC and JNCC-A under the 160th Signal Brigade.

The collapse of the Afghan communication network will be a controlled and deliberate process under a single C2 structure. The retrograde lines of effort created within SROC-A and TF SIGNAL ensure a controlled and repeatable process giving predictability to users, and transparency to stakeholders in Afghanistan.

COL Linda Jantzen TF Signal commander states, "Signal Retrograde Operations represents successful collaboration and cooperation of the entire Signal community in Southwest Asia. The SROC-A simply provides a rally point for that collaboration. We have a process that has been forged in fire and an outstanding team to implement it!"

LTC Jeffrey Thompson *is currently a branch chief within Architecture Operation Networks and Satellites of HQDA CIO/G6. His previous assignments include Joint NetOps Control Center-Afghanistan director and Signal Retrograde Operations Center-Afghanistan director in 2012-13.*

COL Linda Jantzen *has has served in multiple assignments worldwide including 2nd Infantry Division in Korea; 10th Mountain Division at Fort Drum, N.Y.; Combat Maneuver Training Center in Hohenfels, Germany; 22nd Signal Bde in Darmstadt, Germany; 3rd Signal Brigade and 1st Cavalry Division at Fort Hood, Texas; 40th ESB in Ft Huachuca, AZ; Office of the Chief, Legislative Liaison, HQDA, the Pentagon; and 160th Signal Brigade, Camp Arifjan, Kuwait. Her operational deployments include Operation Desert Storm, Operation Restore Hope, Operation Joint Endeavor, Operation Iraqi Freedom II and 07-09, and Operation Enduring Freedom. She is currently in command of 160th Signal Brigade.*

Acronym QuickScan

ARCENT - Army Central Command
BRAC - Base Realignment and Closure
C2 - Command and Control
CENTCOM - Central Command
CMRE - CENTCOM Material Readiness Element
DKETs - Deployable KU-band Earth Terminals
DSST - Direct Signal Support Team
DNS - Domain Name System
DHCP - Dynamic Host Configuration Protocol
EAD - Echelon above Division
ESB - Expeditionary Signal Battalion
FOB - Forward Operating Base
FOI - Found on Installation
GFE - Government Furnished Equipment
IT - Information Technology
ISAF - International Security Assistance Force
JNCC-A - Joint Network Control Center-Afghanistan
JNCC-I - Joint Network Control Center – Iraq
LoE - Line of Effort
MLoS - Microwave Line of Sight
NTOP - Network Optimization Plan
NETCOM - Network Enterprise Technology Command
NATO - North Atlantic Treaty Organization
OEC - Operation Enduring Freedom
OMDAC-SWACA - Operations, Maintenance and Defense of Army Communications in Southwest Asia and Central Asia
RNOSC - Regional Network Operations and Security Center
RS - Resolute Support
SROC-A - Signal Retrograde Operations Center-Afghanistan
SWACC - Southwest Asia Cyber Center
TCF - Technical Control Facility
TPE - Theater Provided Equipment
TLA - Top Level Architecture
TMRs - Transportation Movement Requests
USFOR-A - U. S. Forces-Afghanistan

A step toward the Joint information environment

Main communications facility start-up

By LTC Pam Boyle and MAJ Jacob Cox

(U.S. Army photo by MSG Bruce Brim)

Representatives of the agencies involved in the Main Communications Facility construction were on hand 14 January 2014 at Camp Arifjan, Kuwait, for the official ribbon cutting ceremony. Among those taking part in the ceremony are (left to right) LTC James Riley, 54th Signal Battalion commander; COL Debora Theall, Installation Information Infrastructure Communications and Capabilities project manager; LTC Mollie Pearson, Power Projection Enablers product manager; COL Linda Jantzen, 160th Theater Strategic Signal Brigade commander; Douglas Wiltsie, Program Executive Officer, Program Executive Office for Enterprise Information Systems; MG Wayne Brock, 335th Signal Command (Theater) commander; CSM Bobby Williams, 160th TSSB; BG Christopher Kemp, 335th SIG CMD (T) (P) commander; CSM Charles Mathews, 335th SIG CMD (T) (P); BG Garrett Yee, 335th SIG CMD (T) (P) incoming commander; Daniel Bradford, NETCOM senior technical director; and Larry Klooster, DISA vice principal director. .

In what is being called the first step toward establishing the Joint Information Environment in Southwest Asia, the Main Communications Facility was officially opened with a ribbon-cutting ceremony at Camp Arifjan, Kuwait, on Jan. 14, 2014. This ceremony marked the conclusion of a long and arduous venture to increase command and control, data security, network efficiency, and performance capabilities within the Information Technology infrastructure located at Camp Arifjan, Kuwait.

The 20,000-square-foot facility was a multi-year effort representing the work of numerous personnel and organizations within the Signal Regiment, according to remarks by BG Christopher Kemp, commanding general, 335th Signal Command (Theater) (Provisional) during the ceremony. Representatives from the Defense Information Systems Agency, Program Executive Officer-Enterprise Information Systems, U.S. Central Command, Army Central Command), U. S. Army Network Enterprise Technology Command, and the lead contractor, Program Manager Power Projection Enablers were in attendance. The 335th Signal Command (T)(P) G3 section oversaw the project from its inception.

The 335th Signal Command (T)(P) served as the MCF project lead throughout the migration. The 335th provided funds for equipment purchases and worked with P2E to ensure project deliverables were provided in time to prepare the Operations and Maintenance community for each phase of the migration plan. The unit also worked through unforeseen interruptions including power outages, flooding, and two fires on Camp Arifjan to keep the project moving forward with in accordance with their projected timelines. The 335th also hosted the majority of the synchronization meetings to ensure that key personnel were prepared for each new phase of the migration plan.

While P2E provided oversight for this project, Camp Arifjan's Engineering and Integration and O&M communities shouldered many of the heavy lifts required to see this project to completion. For example, the MCF contract did not include a requirement for contract awardees to relocate Government Furnished

(Continued on page 62)

(Continued from page 61)

Equipment from the previous site to the new facility. Similarly, contract awardees had limited knowledge of the current services offered by the old facility or how their migration plans might affect customer units.

Other limitations surfaced as migration dates approached as well. For example, the ever evolving nature of the SWA network and rapid rotation rates of government personnel at Camp Arifjan provided some complications. For the migration, this met that site surveys conducted by P2E a year prior were no longer accurate once the migration started.

Additionally, these efforts began with almost all Soldiers and contractors on Camp Arifjan being newly introduced to the project.

Still, the greater hurdle to achieving Full Operational Capability for the MCF involved the requirement that migration of all services occur while in production. An entire network structure had to be migrated while customers (warfighters and supporters) continued to use it. As a result, significant planning was required to eliminate, or at least mitigate, service interruptions to customers dependent on these services for command and control. These challenges required that multiple organizations band together with P2E to ultimately achieve FOC. Those organizations included 335th Signal Command (Theater) (Provisional), 160th Theater Strategic Signal Brigade, Southwest Asia Cyber Center--Tier 1 O&M, and 54th Regional Node Operation Support Center--Tier 2 O&M. Each of these organizations greatly contributed to the successful achievement of FOC for the MCF. Within the organizations, the primary leads for the project included LTC Pam Boyle and CPT Asheesh Nikore from 335th Signal Command (T) (P); MAJ Jacob Cox, Ali Alsrogy and David Lucero from SWACC; CPT Steve Yi and CPT Grant Matthews from 160th TSSB; and CPT Raymond Blockmon, CW3 Rylan Knight, and CW2 Jarod Brown from 54th RNOSC.

The SWACC, consisting of Soldiers and contractors responsible for the O&M of enterprise services throughout Southwest Asia, facilitated hundreds of circuit cutover and server migrations.

Additionally, Soldiers moved intrusion detection systems, host based security system servers, Voice over Internet Protocol devices, firewalls, routers, and other critical systems to the new facility. SWACC technicians also completed the transfer of the Southwest Asia Black Core Network solution, a bulk encryption data transport service capable of carrying data from multiple enclaves, to the new facility. For Southwest Asia, the BCN serves as a transport for Secret Internet Protocol Routing, Non-Secret Internet Protocol Routing, Combined Enterprise Regional Information Exchange System, and various other network data simultaneously. Finally, the SWACC also worked to build multiple data paths, such as Generic Routing Encapsulation tunnels, in advance of migrations to facilitate the seamless transfer of services as circuits were cutover to the MCF all throughout the migration. For an organization that typically sees upwards of 200 maintenance tickets each week in addition to many other project initiatives for the theater, the MCF engendered herculean efforts by the Soldiers and contractors of the SWACC.

Similarly, the 160th Signal Brigade and 54th RNOSC oversaw the critical roles of site security and equipment accountability. Ultimately, it was the 160th Signal Brigade who took ownership for the building and the equipment within it. As a result, much of the physical inspecting was completed by technical controllers working for the 54th RNOSC. Much like the SWACC, the 54th RNOSC, is responsible for the O&M of networks, but at the site level (Tier 2), and paralleled many of the efforts performed by the SWACC. Their efforts included transferring government owned equipment such as Tactical Local Area Network Encryption and encryption devices to the MCF and overseeing and inspecting the physical cutover of circuits. Since, the 54th RNOSC also provides local area

network (Tier 2) support to sites across the U.S., Kuwait, and multiple other countries, their efforts to stand up encrypted communications between these sites was imperative to achieving FOC.

Working together, the disparate groups were able to successfully complete an extremely diverse and demanding project.

"It speaks volumes to the quality of our Soldiers, Airmen, civilians and contractors, and their ability to team and deliver in a very complex environment," said BG Christopher Kemp, 335th Signal Command (T)(P) commander.

The MCF includes about 9,000 square feet of space for information technology equipment capable of multiplexing and de-multiplexing circuits transported over copper, fiber, satellite or terrestrial Line of Sight radios. It will serve as the Information Systems hub for Southwest Asia.

"The MCF is a secure, self-contained facility that will serve as the IT hub for Southwest Asia," said Douglas K. Wiltsie, Program Executive Office Enterprise Information Systems commander. "This effort is the first step toward the JIE for CENTCOM, which has an area of responsibility for 20 countries from Afghanistan and Bahrain, to Egypt, Iran, Uzbekistan, and Yemen.

Prior to the MCF, Camp Arifjan housed most of its circuitry in a former maintenance bay. The systems included legacy, ad hoc and a host of patched together networks, some of which had not been used in years.

The Southwest Asia theater network supports 19 Countries in the CENTCOM Area of Responsibility and four network enclaves, yet the communication facility's previous environment suffered from years of ad-hoc initiatives undertaken to support multiple, urgent and varied theater requirements. Little regard was given to a change management process. Consequently, requirements quickly outgrew the previous site's capability to support the theater's growing footprint in Southwest Asia. The result was a costly facility suffering HVAC, power, and capacity issues presenting a high risk of data loss and or corruption. To correct these deficiencies, P2E, on behalf of the government, initiated a contract on14 September 2012 to complete the MCF and transfer current services to the new facility. Notably, this was the largest project P2E has ever attempted.

"Theater communications architecture has previously been limited by the ad hoc way in which it was built over the years," said COL Linda Jantzen, 160th TSSB commander. "Our technical control facilities were characterized by a lack of standardization, inefficient and disparate power and cooling systems, localized data and service delivery, out of life cycle components, and duplication of effort. The implementation of the MCF reset a large portion of the Army's critical communications assets within the theater while introducing scalability (increased physical space, HVAC, power, and digital storage) for future requirements across Southwest Asia.

"In addition to giving us a much better quality facility at Camp Arifjan, the MCF migration has created an information systems hub for the theater, with the technology and storage capacity to host services for users across the theater, leverage Enterprise services, and support future growth," COL Jantzen said. "This brings us in line with Army and DoD modernization efforts and makes us much more secure and efficient in many ways – by reducing the physical footprint, reducing hardware and sustainment requirements, reducing the overall administrative burden through enabling centralized patching and vulnerability remediation, and by increasing security and scalability of the network."

Setting and resetting the theater is a vital part of the MCF's mission. The new facility will increase the data storage capacity exponentially due to virtualization.

"We now have the capability to provide the theater with the critical space necessary to support emerging programs, such as DISA's JRSS, and to assist the theater with meeting the JIE construct," COL Jantzen said. "The virtual

(Continued on page 64)

(Continued from page 63)

infrastructure increases the theater's capability by providing a total of 3705 TB of storage space, making it possible to scale to theater service/server requirements without requiring any additional hardware for years to come. In addition, we have steadily built up our transmission paths and bandwidth over the years and we can now make use of that to support multiple sites across the theater with service delivery and replication."

The MCF is the corner stone for the construction of the Joint Information Environment. The Technical Control portion of the MCF will host DISA's Tier 0 Internet Protocol access, along with the future home of one of three Joint Regional Security Stacks that will be deployed to the theater.

"Without a doubt, the Camp Arifjan MCF will have a significant impact on laying the foundation for the Joint Information Environment, or JIE, as well as being a critical component for all of our future activities in the region," Wiltsie noted. "JIE is an important vision for the Department and requires seamless teamwork across the Services to archive success. We are already working with our partners across the Army, Navy, Air Force, Marine Corps and DOD to make the incorporation of the separate Service networks within the DOD into a shared architecture a reality, and the MCF is the first step. Expected to reach full capability between 2016 and 2020, the JIE will enable all DOD personnel to access the network from any approved device, anywhere, and at any time in order to communicate securely and reliably. The JIE will provide full-spectrum support to the operation, procurement, and maintenance of IT systems.

"The Camp Arifjan MCF provides enhanced forward capability to support JIE for the CENTCOM Commander," he continued. "The MCF also supports strategic COOP initiatives for Mission Command Nodes and serves as a prototype model to emulate and capture lessons learned across global strategic networks. It supports strategic diversity between Bahrain, Qatar, and Camp Arifjan, and is a global access point in support of DISA architecture."

The 335th Signal Command (T)(P) oversaw the project, starting with planning in 2009. Once the building was completed in 2012, planning began to move several hundred circuits, government-furnished equipment, and new systems, such as the JRSS. That phase is largely complete, although new systems will continue to be installed and upgraded as necessary. The facility is currently operated and maintained by the 160th TSSB.

"Our role is to operate, maintain, and secure not only the transmission systems and server stacks, but the facility itself," COL Jantzen said. "In addition to taking care of the building and the equipment housed in it, we have to ensure all of that capability is translated into better service and mission success for our customers. The MCF postures the brigade to provide the necessary resources to host and meet the needs of emerging technologies. It also enables us to continue supporting critical theater communications infrastructure such as ARCENT and U.S. Forces Afghanistan as we transition the theater from fighting two major conflicts to a more steady state. The customer should not care where their data is housed or where their services are pulled from, and they won't care as long as it is reliable and available when they need it. The Southwest Asia Cyber Center and 54th Signal Battalion have learned and adapted to the new technology and added personnel with new skill sets that have postured us for the current mission as well as preparing for the future."

The MCF will continue to affect communications throughout Southwest Asia, and will serve as a model for similar facilities in Germany and Hawaii.

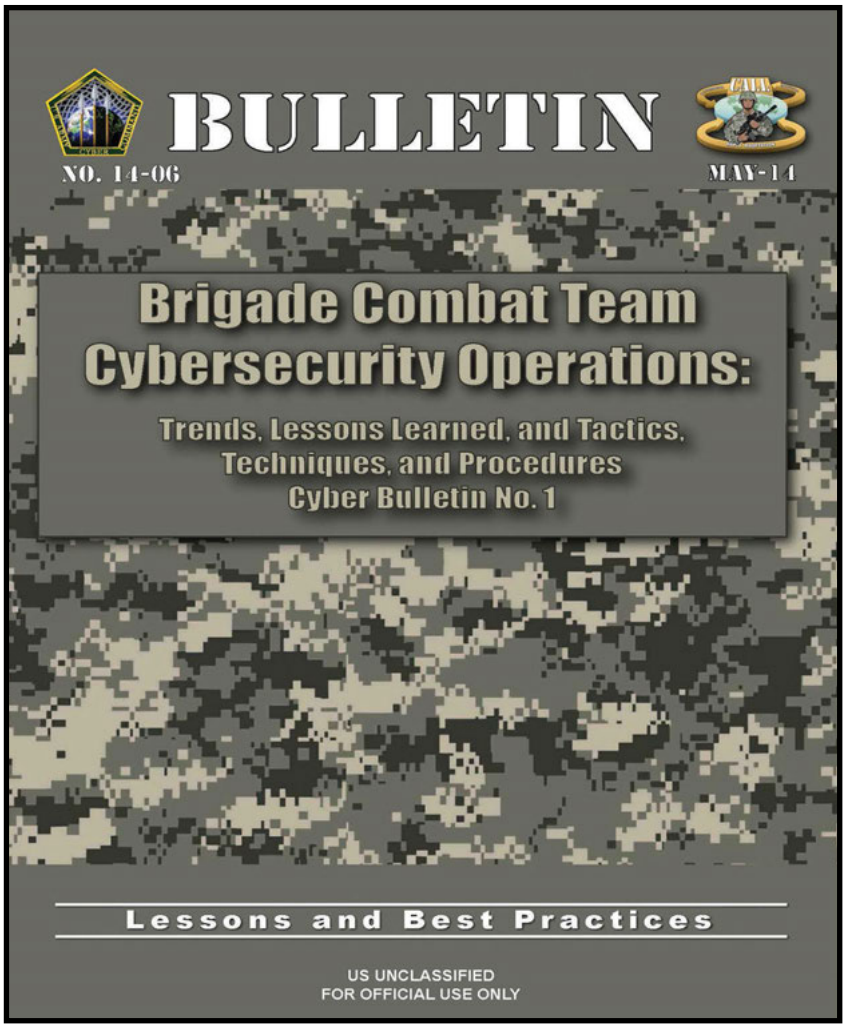
"I am really proud of the work that the team 335th Signal Command (T)(P), NETCOM, G6 and the PM P2E did to accomplish this mission," Wiltsie said. "Their success has resulted in a state-of-the-art MCF dedicated to supporting forward deployed personnel despite austere and arduous working conditions inherent to the SWA region, numerous long hours over holidays

and weekends, multiple stakeholders, and technical complexities. The team was able to overcome these challenges and still coordinate all activities regardless of the eight hour time zone difference between Kuwait and Fort Belvoir, Va."

LTC Pam Boyle *is the chief of operations for the 335th Signal Command (Theater) (Provisional) at Camp Arifjan, Kuwait. She holds an associate's degree in computer science degree from Hawaii Pacific University, a bachelor's and master's degree in journalism from the University of Montana, and master's degrees in cybersecurity policy and information assurance management from the University of Maryland University College. She is currently pursuing her doctorate in information assurance from Capitol College in Maryland.*

MAJ Jacob H. Cox Jr*. is a telecommunications systems engineer currently serving as the chief enterprise operations officer for the South West Asia Cyber Center, Camp Arifjan, Kuwait. He holds a bachelor of science in Electrical Engineering from Clemson University and a MS Degree in electrical and computer engineering from Duke University, N.C. MAJ Cox is a selectee to pursue a Ph.D. in electrical and computer engineering at Georgia Institute of Technology starting August 2014*

Cyberspace Lessons Learned Bulletin 14-06



The Mission Command Center of Excellence at the U.S. Army Combined Arms Center, Fort Leavenworth Kan., has released the first in a series of e-bulletins aimed at integrating cyberspace operations and cyber-electromagnetic activities into the U.S. Army organizational culture, operations and procedures. The bulletins will concisely convey TTPs Army units should leverage to counter the pervasive and increasingly sophisticated cyberspace threats which exist in the current and future operational environment. This inaugural issue focuses on cybersecurity (formerly Information Assurance) best practices that BCT commanders can employ to enhance their unit's performance, including the considerations of computer network defense, insider threats and social media concerns.

https://call2.army.mil/

DEPARTMENT OF THE ARMY
ARMY COMMUNICATOR
USASC&FG
ATTN: ATZH-POM
Fort Gordon, Georgia 30905-5301

OFFICIAL BUSINESS
ISSN 0362-5745

PERIODICALS
Postage and fees paid
at Augusta, Georgia and
additional cities

CYBER NETWORK DEFENDER

25D

Protects against, monitors for, performs analysis of, responds to and detects unauthorized activity in the cyberspace domain, which includes deployment and administration of the infrastructure; performs deliberate actions to modify information systems or network configurations in response to threat information; collects data gathered from a variety of CND tools to analyze events and warn of attacks that occur within the environment. Performs the duties associated with the five Computer Network Defense (CND) specialties (i.e., Infrastructure Support (IS), Analyst (AN), Incident Responder (IR), Auditor (AU) and Manager (MGR)), Information Assurance Technical (IAT) Levels I-III functions, Information Assurance Management (IAM) Levels II-III functions, as required by skill level IAW AR 25-2 and DoD 8570.01-M, and Communications Security (COMSEC) Account Management (CAM) IAW AR 380-40.

ARMY COMMUNICATOR

Signal Towers, Room 713
Fort Gordon, Georgia 30905-5301
PIN: 104445-000