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

ARMY COMMUNICATOR

Voice of the Signal Regiment PB 11-12-2 2012 Vol. 37 No. 2

MOBILE COMPUTING

Smaller Systems, Bigger Solutions.

PLUS:

- The Army Software Marketplace
- Applications and Cellular Testing at the NIE
- DOD's Mobility Requirements

CHIEF OF SIGNAL

Alan R. Lynn

Mobile computing here-and-now with both benefits and challenges

Leaders,

Mobile computing is not the future --it is happening today and the security issues of this type of computing are the only things we are wrestling with as we continue to test the boundaries of both commercial and tactical mobile computing.

I see a future where we will use military frequency spectrum and commercial spectrum to provide unprecedented throughput in mobile computing. I see our posts, camps and stations in the future being totally wireless with the exception of a few emergency wired systems. We will have more opportunities for telecommuting in the future but we have to start today by walking away from paper. If all our systems are "paperless" or "digital" then there is nothing that is holding us to brick and mortar buildings. Here at the Signal Center we operate in a digital environment. We sign and move our documents digitally (unless it is an award that will end up on someone's wall--a keepsake). Please take on this challenge as well—It's important to start today!

The Signal Regiment is filling a leading role towards making mobile computing a reality. We are testing commercial mobile computing systems with our tactical networks in the Network Integration Evaluation at Fort Bliss and pushing the envelope on what is possible.

Here at the Signal Center of Excellence, we are also working within TRADOC's Connecting Soldiers to Digital Applications effort to ensure the processes, standards, and governance pieces are designed to meet the Warfighters' needs. CSDA is led by the Mission Command Center of Excellence at the Combined Arms Center, and the SIGCoE has been an integral player in this effort over the past two years.

CSDA includes four focus areas: (1) Device/Network Access, the development of four specific mobile environments in coordination with NSA, DoD CIO, DA CIO/G-6, and ASA(ALT)/PEO Soldier; (2) The Army Marketplace, the coordination with the DA CIO/G-6 to develop a functional Army Apps Marketplace; (3) TRADOC Policy, the documentation of Apps development, validation and management ICW with TRADOC G 3/5/7, TCM dL, and DA CIO/G-6; and, (4) Concept Exploration, the continuation of Apps development and mobile apps pilot programs within the TRADOC Centers of Excellence.

Central to this effort has been our ability to create meaningful, mobile applications to meet the Warfighters' needs while keeping an eye on the vulnerability issues surrounding mobile and wireless computing. As of this date, our small team within the SIGCoE has created nearly 100 unclassified mobile apps for Android and iOS platforms, resulting in over 1.5 million downloads. To find these apps on the Android Market or iOS App Store, simply search for "fa53" and the free apps from the Signal Center of Excellence will appear. Bugle Calls, Soldier's Blue Book, Signal Lieutenant Handbook, Physical Readiness Training, Army Values, APFT and Body Fat Calculator, and Router Training Guide are just a few of the apps available online from the SIGCoE.

In this edition of the Army Communicator, we explore the future of mobile computing in the Army while looking at the OPSEC and security issues prevalent in the wireless communications arena. I encourage you to read the articles in this issue to stay informed on this highly relevant topic!

For the Nation!

Join the Discussion
https://signallink.army.mil

U.S. Army Signal Center of Excellence
Fort Gordon

Command

Chief of Signal
MG Alan R. Lynn

Regimental Chief Warrant Officer
CW5 Todd M. Boudreau

Regimental Command Sergeant Major
CSM Ronald S. Pflieger

Editorial Staff

Editor-in-Chief
Larry Edmond

Art Director/Illustrator
Billy Cheney

Photography
Billy Cheney, SSG Joshua Ford, General Dynamics, Bonnie Heater, SGT Michael J. MacLeod, Claire Schwerin, Amy Walker, Nick Spinelli

By Order of the Secretary of the Army

Raymond T. Odierno
General, United States Army
Chief of Staff

Official:
JOYCE E. MORROW
Administrative Assistant to the Secretary of the Army

Authorization 1214501

Army Communicator (ISSN 0362-5745) (USPS 305-470) is published quarterly by the U.S. Army Signal 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 Signal 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 Signal Center of Excellence, Signal Towers (Building 29808), Room 713, Fort Gordon, Ga. 30905-5301.

CORRESPONDENCE: Address all correspondence to *Army Communicator,* U.S. Army Signal 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.

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

PB 11-12-06
Summer 2012
Vol. 37 No. 2

Army Communicator

Voice of the Signal Regiment

Table of Contents

Features

This edition covers the state of mobile computing and some of the security issues involved.

Cover: *This edition delves into the rapidly changing landscape of mobile computing where capabilities are growing exponentially as the size of systems continue shrinking.*

Cover by Billy Cheney

Join the Discussion

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

REGIMENTAL CWO Todd M. Boudreau

Mobile technology revolution underway

Signaleers,

First, please allow me to communicate a hardy Army HOOAH to soon to be promoted LTG Via, our first Signal four-star general officer. Go Signal! This is truly an exciting time in the history of the Army Signal Corps.

This edition of the *Army Communicator* presents more history in the making; the emergence and integration of mobile computing devices and applications into the Department of Defense communications infrastructure and our LandWarNet. What was once just a prop in a popular science fiction television series has now become a game-changing capability to extend mission command.

According to Wikipedia, 'throughout Star Trek Enterprise and The Original Series, on-ship communication is achieved via communicator panels on desks and walls, and sometimes through the use of videophones. While on away missions, the crew carried hand-held communicators that flip open. The top section contains a transceiver antenna and the bottom contains user controls, a speaker and a microphone.'

Although we still do not have a handheld device yet that can "use subspace transmissions that do not conform to normal rules of physics [and] can bypass EM interference [in order to] allow nearly instantaneous communication at distances that would otherwise require more time to traverse," we seem to have beat our Trekkies' heroes in that we are not only able to move voice traffic via a handheld device, but also data as well as still and moving imagery. In fact, herein lies the power of such devices; digital applications that bring actionable intelligence and powerful capabilities to the point of need to enable an overwhelming advantage to our planet's most powerful professional warriors.

Unfortunately, many misunderstand the necessity to carefully integrate these devices and applications under approved processes, proven standards, and structured governance. While Certificates of Networthiness, Army marketplace governance, Federal Information Processing Standard certifications, and Security Technical Implementation Guides are often seen as obstacles to progress, we must help our customers understand their necessity; many do not understand that almost any weakness introduced at almost any location within our LandWarNet has the ability to infect an area well outside the physical location of the vectored vulnerability. And since we seem to have moved past technology enabled to technology dependant, such an infection could result in grave loss, to include loss of life.

It can be likened to the public use of rivers and streams for water and waste. If you own land across which such a source of water flows, you might feel that you have a right to draw upon that water and pump your waste into it as well. You might even take offense or at a minimum be frustrated at the myriad of paperwork you are made to complete just to connect to your own water. However, you begin to think quite differently when you hear of a neighbor's desire to connect his septic tank to this same stream; especially since this neighbor happens to live upstream. In a domain where, for all intents and purposes, everyone is upstream, we must ask ourselves, is it not extremely important what gets connected to our source of life?

This and many other aspects of mobile computing are addressed in this edition. Additionally, we solicit your thoughts, expertise, and support in integrating these game-changing technologies into our warfighting efforts. And as always, thank you for your dedication and service in being ever Watchful for Our Country.

Pro Patria Vigilans!

REGIMENTAL CSM

Ronald Pflieger

Vunerabilities come with mobile 'smart' devices

Signaleers,

Mobile computing is everywhere. Both on and off duty, tablets, Smartphones, laptops and other portable devices have been injected into the very fabric of our lives. Rarely do you see someone walking around without a Smartphone or tablet in hand – especially if that person is under 20 years old. Our culture has changed and continues changing in order to accommodate the mobile computing paradigm.

The Army culture is moving in that direction as well. While many leaders are justifiably worried about the inherent vulnerabilities within wireless communication, the benefits of using tablets and other like devices push us to find better ways of allowing these devices on our networks.

Right now, in order to connect Smartphones and tablets to military networks, an approved solution will have to meet four criteria: FIPS 140-2 validated crypto; approved data-at-rest; Common Access Card enablement; and, enterprise management. Currently, only tablets running the Windows 7 Army Gold Master software package and the BlackBerry Playbook meet those standards. While this is a step in the right direction, we need to do better.

The Signal Regiment is at the forefront of this movement to allow more smart devices on our networks. The Regiment's leaders realize that enabling the Army to achieve its mobile computing requirements is an important step forward. Signal NCOs and Soldiers will continue to be at the center of this transformation.

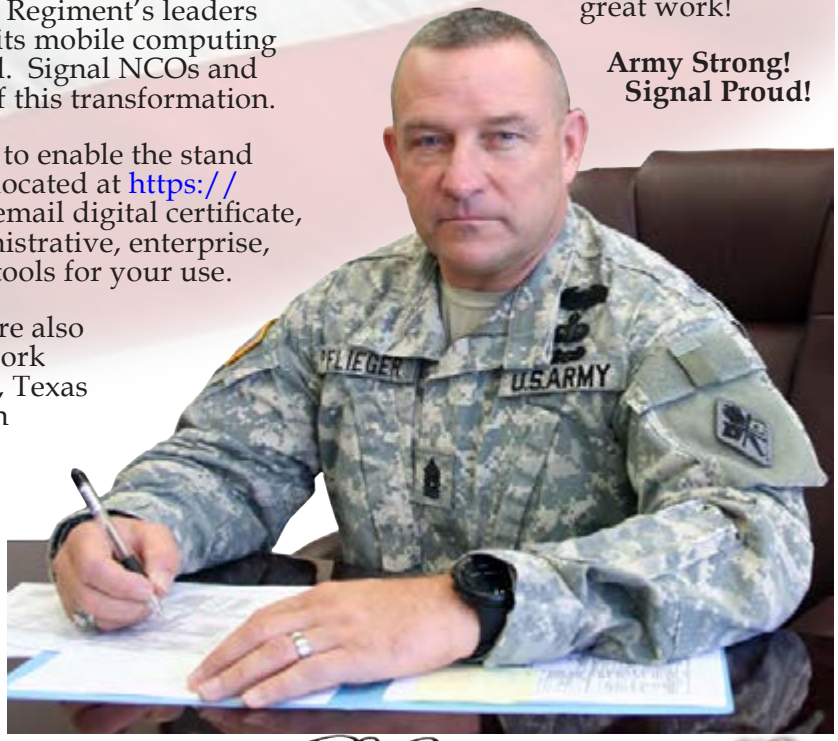
We are working with the Army's CIO/G6 to enable the stand up of their prototype Army MarketPlace, located at https://marketplace.army.mil/. Using your non-email digital certificate, you can access this site and find the administrative, enterprise, training, productivity, and other types of tools for your use.

The Regiment's NCOs and other leaders are also actively engaged in the twice-yearly Network Integration Evaluation events at Fort Bliss, Texas where an active-duty brigade combat team conducts exercises considering all aspects of network capabilities in an austere environment. The evaluations occur from platoon levels all the way up to brigade level itself. NIE also serves as a test bed of sorts to look at systems under test (e.g., WIN-T) and systems under evaluation. NIE is a comprehensive exercise that serves as the centerpiece of network integration in the Army today.

Leaders at the U.S. Army Signal Center of Excellence are also working to expand the use of mobile devices for our Soldiers' and NCOs' training and education. Currently, we use quick response codes on assemblages to allow students to download mobile training content and the associated equipment. We hope to expand this capability across the board soon.

The Regiment's continued success in mobile computing and advanced networking is directly a result of the great efforts by our leaders and Soldiers on the ground. Keep up the great work!

Army Strong!
Signal Proud!



The road to four stars

Signal Corps milestones

By Steven J. Rauch

The announcement that LTG (P) Dennis L. Via has been nominated for promotion to the rank of general marks an important milestone in the history of the U.S. Army Signal Corps.

LTG Via's promotion will make him the highest ranking Signal Corps officer in the branch's 152- year history. Once promoted, LTG (P) Via will join the ranks of three other Signal officers who broke through a general officer rank barrier during the course of Signal Corps history.

After the founding of the branch in 1860, 20 years elapsed before the founder of the Signal Corps Albert J. Myer achieved the rank of brigadier general on 16 June 1880.

Twenty-six years later, Adolphus W. Greely attained the rank of major general in 1906. He went on to assume command of Army organizations outside of the Signal Corps. In 1958 a Signal officer advanced to the next level when MG James D. O'Connell, who had become the 19th Chief Signal Officer in 1955, attained the rank of lieutenant general, 52 years after MG Greely's achievement.

The position of Chief Signal Officer remained, however, a two-star billet. The post held by the Army's chief communications officer would not permanently attain a three-star rank until its designation as the assistant chief of staff for information management in 1984. Since 1958, due to numerous reorganizations of U.S. Army force structure, it has long been a possibility that a Signal officer would achieve the rank of four-star general. Now some 54 years after the first Signal Corps lieutenant general was appointed; an exceptionally distinguished Signal officer will attain the Army's highest current rank.

As the commanding general of U.S. Army Materiel Command, LTG (P) Via will become the senior logistician for the U.S. Army, a position for which he has been prepared in his capacity as AMC deputy commanding general since 1 May 2011.

As commanding general, his duties will encompass a broad array of responsibilities ranging beyond dealing primarily with Signal- related issues.

Given this historic event, it is worth studying those officers who attained each general officer rank for the first time as well as the organizational changes which paved the way for the next rung which LTG (P) Via will attain upon his promotion to general.

BG Albert J. Myer

For many years Albert J. Myer was the only officer and member of the organization known today as the Signal Corps. On 27 June 1860, Myer was appointed to the position of Signal Officer of the Army (a staff position akin to that of Army G-6 today) by President James Buchanan.

At the time, the Army authorization documents reflected only one position for a Signal officer, thus Myer was truly a "Signal Corps of One." During the first half of the Civil War, additional personnel were obtained for Signal duty through a branch detail of officers and Soldiers from infantry, artillery, and cavalry regiments to serve as "acting" Signal officers, sergeants, and Soldiers. However, this detail system made for a very uncertain structure.

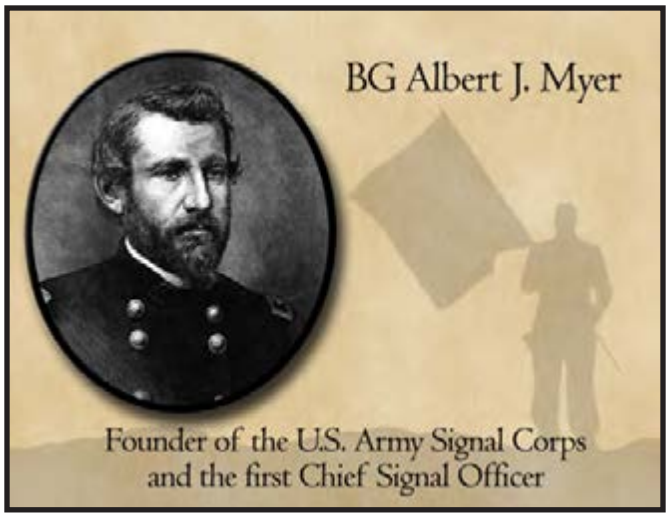
Finally in March 1863, Congress passed legislation to authorize a separate and distinct structure for Signal Corps personnel, to include authorizing the senior position of the branch to be titled Chief Signal Officer, with the rank of colonel.

For a brief period during the Civil War, Myer held the position as colonel under a recess appointment by Congress. However in 1863 he was relieved from the position by Secretary of War Edwin M. Stanton for failing to obtain authorization to hire licensed civilian telegraphers for the Signal Corps.

When his commission as colonel expired without action, Myer reverted to his permanent rank of major, while other officers assumed the duties and position of Chief Signal Officer. After the Civil War when the Army reorganized in 1866, Congress authorized a small Signal Corps.

Myer solicited the support of LTG Ulysses S. Grant, then commanding general of the Army, for reappointment to the Chief Signal Officer position. Myer was reinstated in 1866, and held the position at that rank until the twilight of his career.

Historical records, however, reflect Myer using the rank "Brevet Brigadier General" on correspondence throughout the period. He did so because he had been awarded the brevet rank on 13 March 1865 for organizing and training



the men of the Signal Corps during the war. The award of a brevet accorded officers permission to wear and use that rank in correspondence. But they continued to be paid at their lower permanent rank. Thus documents signed by Myer during his career reflect his status as a brevet brigadier general, and he was referred to as "General Myer" by officers and Soldiers.

In 1880 the U.S. Army reorganized again and as a result several branch chiefs' positions were increased to the rank of brigadier general. War Department General Orders No. 57, dated 2 July 1880, authorized a Signal Corps budget of $375,000 for Fiscal Year 1881, added 50 privates to the force structure, and increased the rank of Chief Signal Officer to brigadier general.

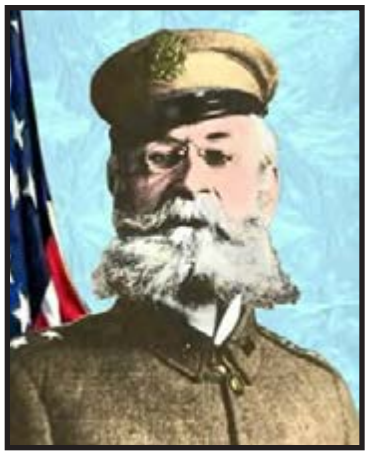
Thus Myer was promoted to the rank of brigadier general with an effective date of 16 June 1880. Unfortunately, Myer did not enjoy much time to savor the accomplishment due to his death from nephritis on 24 August 1880 at the age of 51.

MG Adolphus W. Greely

Beginning with his service as a volunteer Soldier during the Civil War, Adolphus W. Greely established a stellar career as one of the few officers serving in the post-war Signal Corps. From 1866 to 1887 Greely proved himself to be a diligent, adaptable and demanding leader. His most notable exploit was his arduous mission to conduct weather research in the Arctic Circle as commander of a 24-man expedition from 1881 to1884. Despite the terrible hardships and the loss of 19 of his men, LT Greely brought back all of the expedition's records containing important meteorological observations. In June 1886, at the age of 42, he was promoted to captain in the Regular Army after serving 19 years as a first lieutenant. Upon the death of Myer's successor BG William B. Hazen in 1887, the well-known Greely received the coveted appointment to Regular Army brigadier general and the position as Chief Signal Officer of the U.S. Army in March 1887. For the next 19 years Greely would enthusiastically lead the Signal Corps during a challenging Army paradigm shift from a continental focused organization to that of an expeditionary Army of a growing international power.

Greely's performance as Chief Signal Officer during the Spanish–American War established his reputation in the minds of the nation's leaders, particularly President William McKinley and his successor, President Theodore Roosevelt. Thus on 10 February 1906, President Roosevelt promoted Greely to major general making him the first Signal officer to achieve that rank. He was then assigned to command the Department of the Pacific, one of several geographic commands of the U.S. Army, with responsibility for command and control of all Army units and organizations within the area. This promotion marked a milestone for an officer who had spent almost his entire career within a technical service but who was seen as possessing the universal qualities required to command one of the Army's geographic areas.

Greely had barely pinned on his second star when he was presented with the challenge of the great San Francisco earthquake on 18 April 1906 which devastated that city. As department commander, Greely was responsible for the recovery and relief efforts, to include the repair and restoration of communications systems.


MG Greely

To accomplish this mission he made use of one of the Army's first automobiles to enable faster hauling of supplies, food, the sick and wounded and anything else that needed to be moved. Greely was subsequently assigned as commander of the Northern Division and ended the Ute Rebellion in 1906 without bloodshed. His final assignment was command of the Department of the Columbia.

Thus Greely proved to be a leader far beyond the traditional role of a Signal officer. Greely retired from the Army in 1908 and enjoyed a long and productive retirement. On his 91st birthday, 27 March 1935, he was awarded a special Medal of Honor for his many contributions to the nation during his long career. He died on 20 October 1935 at Walter Reed Hospital and was

(Continued on page 6)

(Continued from page 5)

buried with full honors at Arlington National Cemetery.

LTG James D. O'Connell

In May 1955 MG James D. O'Connell assumed the position of 19th Chief Signal Officer of the U.S. Army. O'Connell was a 1922 West Point graduate who was commissioned into the infantry. After initial assignments to posts in Michigan, O'Connell attended the Signal School at Camp Alfred Vail (later Fort Monmouth) N.J. Upon graduation in June 1925 he was assigned to duty with the 35th Infantry as the regimental communications officer (S6).

LTG O'Connell

He later was assigned to the 24th Infantry but in December 1928 he returned to the Signal School as an instructor. On 31 May 1929 he transferred to the Signal Corps. In August 1929 he entered the Sheffield Scientific School at Yale University where he graduated with a Master of Science in communication engineering in 1930.

During the 1930s and 1940s, O'Connell served in a variety of assignments related to communications technology at the Signal Corps laboratories at Fort Monmouth. In 1941 he was appointed head of radio communications projects in the office of the Chief Signal Officer in Washington, D.C. During World War II he served in the Signal section of the headquarters 12th Army Group as the chief communications officer (G6).

After the war he became director of the Fort Monmouth laboratories until 1947 when he was appointed as the signal officer (G6) of the Eighth Army in Korea until 1949.

Upon his return from Korea he served as the deputy Chief Signal Officer from 1951 until 1 May 1955 when he became the 19th Chief Signal Officer.

On 11 July 1958 he was selected for promotion to lieutenant general, the first Signal officer to ever hold that rank.

After his retirement in April 1959, O'Connell spent several years as vice president of the General Telephone and Electronics Laboratories in California. In 1964 he joined the staff of President Lyndon B. Johnson as the special assistant to the president for telecommunications and director of telecommunications management in the Office of Emergency Planning. He died in July 1984 and was buried in Arlington National Cemetery.

Army Reorganizations Pave the Path to four-Stars

In the early 1960s Secretary of Defense Robert S. McNamara directed a thorough review of the Army's organizations and staff relationships.

This resulted in a significant reorganization approved by President John F. Kennedy in 1962 that enacted major shifts in tasks performed by the Army staff and the previously stove-piped organized technical services. In an effort to centralize personnel, training, research and development, and supply operations, most of the technical services were abolished.

The positions of the Chief Chemical Officer, the Chief of Ordnance, and the Quartermaster General completely evaporated. The Chief Signal Officer and the Chief of Transportation continued to perform their duties, but as special staff officers instead of branch chiefs.

Later the Chief Signal Officer obtained a seat on the Army Staff, but was called the Assistant Chief of Staff for Communications-Electronics beginning in 1967.

From 1967 until the present, the Army staff position continually changed names, among which were Director of Telecommunications and Command and Control (1974-1978); Assistant Chief of Staff for Automation and Communications (1978-1981); Assistant Deputy Chief of Staff or Operations and Plans (Command, Control, Communications, and Computers) (1981-1984); Assistant Chief of Staff for Information Management (1984-1987); Director of Information Systems for Command, Control, Communications and Computers (1987- 2002); and Chief Information Officer/G6 (CIO/G6) (2002 – present).

Generally the officers holding this position were lieutenant generals, beginning with LTG Thomas M. Rienzi in 1972. On occasion, however, non-Signal officers would be assigned to this position, thus it was not exclusive to the Signal Corps.

For a short time in 1987, the Signal Corps had six lieutenant generals in various positions throughout the Army. These included LTG Thurman D. Rodgers (ACS for Information Management); LTG Emmett Paige, Jr., (CG, U.S. Army Information Systems Command); LTG Vaughn O. Lang (Deputy Assistant Secretary of Defense for Mobilization Planning and Requirements, OSD); LTG Clarence E. McKnight, Jr., (Director, C3 Systems/Director Joint Strategic Connectivity Staff, JCS); LTG James M. Rockwell (Deputy Director, NATO Communications Information Systems Agency – Outgoing) and LTG Robert J. Donahue (Deputy Director, NATO Communications Information Systems Agency - Incoming).

This constellation of lieutenant

generals reflected how the special leadership skills of Signal general officers were recognized by the nation's leaders and entrusted with positions of responsibility far beyond those of just Army communications.

The road to the next level – four-star general – became possible due to the 1962 reorganization. Most of the functions of the Signal Corps transferred to the US Continental Army Command and to two new commands, the Army Materiel Command and the Combat Developments Command. The impact for the Signal Corps was that the CDC became responsible for Army doctrine; CONARC took over schools and training; and AMC acquired authority for research and development, procurement, supply, and maintenance. Under AMC all Signal-related research, development and acquisition was organized under a sub-command which would evolve through time to become the Communications – Electronics Command or CECOM as it is known today. Thus the commander of CECOM, a major general command, could eventually attain the experience and leadership proficiency which could be applied across the wider scope of the AMC mission. Consequently, a former CECOM commander could advance to become a higher staff officer within AMC or potentially, the AMC commander. Thanks to the 1962 reorganization, a former CECOM commander, LTG (P) Dennis L. Via has now advanced to the point where he will achieve command of an organization he knows well, the Army Materiel Command and thus he will attain the rank of four-star general.

LTG (P) Dennis L. Via

Unlike the predecessors mentioned here, LTG (P) Via's career reflects that of primarily a Signal officer in training and assignments through lieutenant general. Myer had once been an Army surgeon, Greely had once been an infantry Soldier, and O'Connell had been commissioned as an infantry officer. LTG (P) Via is a 1980 graduate of the ROTC program at Virginia State University and has attended the Signal Officer Basic and Advanced Courses, U.S. Army Command and General Staff College, and the Army War College. His assignments began in January 1981 as a signal platoon leader in Company A, 25th Signal Battalion. Following completion of the Signal officer advanced course in March 1986, he was the Chief, Switching Section, Operations Branch and later Aide-de-Camp to the Chief of Staff, Allied Forces Southern Europe in Naples, Italy.

LTG (P) Via Via served as the Operations Officer, J-6, for the Armed Forces Inaugural Committee from June 1988 to March 1989 and then became the assignment officer for Functional Area 49 (Operations Research/Systems Analysis) at the U.S. Army Personnel Command. Following attendance at the U.S. Army Command and General Staff College he served as Assistant Division Signal Officer, 82d Airborne Division and then S3 and XO for the 82d Signal Battalion at Fort Bragg, N.C. He would later command the 82d Signal Battalion from July 1996 to July 1998. Upon graduation from the US Army War College in 1999, LTG (P) Via became the Deputy Assistant Chief of Staff, G-6, III Corps at Fort Hood, Texas and in June 2000 assumed command of the 3d Signal Brigade. From there Via returned to Washington DC where he served in the Army G-8 and then as Director, Global Information Grid Operations/Commander, Defense Information Systems Agency and Global Operations/Deputy Commander, JTF-Global Network Operations, DISA. He was promoted to brigadier general in that position on 1 January 2005.

In August 2005 LTG (P) Via became commander of the 5th Signal Command/Deputy Chief of Staff G-6, U.S. Army Europe and Seventh Army. During his next assignment as the CG U.S. Army Communications-Electronics Life Cycle Management Command, he was promoted to major general on 2 June 2008. LTG (P) Via was promoted to his present rank on 3 August 2009 when he became Director for C4 Systems, J-6, the Joint Staff. In May 2011 he assumed his current position as Deputy Commanding General/Chief of Staff U.S. Army Materiel Command at Redstone Arsenal, Ala.

LTG(P) Via

As LTG (P) Via breaks new ground as a general and commander of AMC, he will no doubt illustrate to the entire Army the superb leadership skills that members of the U.S. Army Signal Corps have been fortunate to have been associated with since his first day in the Signal Officer Basic Course in 1980. Whatever legacy he leaves as a general will become an integral part of Signal Corps history alongside that of Myer, Greely, and O'Connell. He is no doubt up to the challenge. Good luck, LTG (P) Via!

Steven J. Rauch ***is the U. S. Army Signal Branch historian at the U.S. Army Signal Center of Excellence and Fort Gordon, Ga.***

Mobile technologies altering all processes

By BG Randal Dragon and Mike McCarthy

Two years ago U.S. Army leaders embarked on a project assessing the power of Smartphone technology to fundamentally change how Soldiers communicate and access data, knowledge and training. The intent of the project was to determine if there was significant value and military utility in leveraging the quantum advances and rapid developments across the spectrum of Smartphone-related technologies to fill the capabilities gaps identified in the legacy systems of the U.S. Army.

Rather than establish a traditional acquisition program, the senior leadership of the Army provided guidance for the U.S. Army Training and Doctrine Command to establish what became known as the "Connecting Soldiers to Digital Applications" or "CSDA" project. The Army Capabilities Integration Center and its subordinate Brigade Modernization Command at Fort Bliss, Texas were given the lead for establishing and managing the project for TRADOC and the Army. Using a series of low dollar pilot projects, across a broad spectrum of potential use cases in the administrative, training and operational domains for the rapidly advancing technologies of the Smartphone industry, the CSDA initiative began looking for systemic solutions to assess industry solutions.

From the very beginning of the CSDA project, the goals were clearly defined by the senior leadership of the Army. CSDA is intended to define best practices needed to give our Soldiers the advantage of emerging technologies and capabilities. The project identifies and develops new approaches to create a persistent learning environment for the Soldier by adapting existing and emerging technologies. It was also designed to forge a path forward to enable every Soldier access to relevant and critical knowledge, information and learning, independent of the Soldier's location or environment. Additionally, CSDA develops the means to rapidly update and disseminate relevant information at a fraction of the cost of traditional methods. Finally, it arms the Soldiers with select administrative, training, and tactical applications to accomplish individual and collective tasks.

In keeping with a new approach of reviewing and assessing emerging technologies, the CSDA project was given the challenge of using what became known as the Agile Capabilities Life Cycle Process (commonly referred to as the "Agile Process") to reduce the traditional development and acquisition five to seven year process. This abbreviated process offers the Acquisition community a venue to cut through cumbersome administrative policies and practices in order to deliver the best technologies available to the Soldier as rapidly as possible. Rather than establish a special project office full of experts, it was determined that the best approach was to leverage work being done across the Army with various aspects of Smartphone technologies and to integrate Soldier feedback throughout.

An underlying principle for the CSDA project was to seek solutions that could evolve with the continuing innovation and advancements in technology that frames the Smartphone industry. It has always been about more than Apps or hardware; the CSDA project is about finding paths that will enable Soldiers to take advantage of new and emerging technologies – to give them a competitive advantage in combat, training and garrison at the edge. No one has the ability to look far into the future and identify what the most affordable and best technologies will be available in five or ten years, any more than could have been predicted ten years ago.

The CSDA project was structured to look for long-term solutions that provide the best technology the Army can afford. The velocity of change throughout the Smartphone industry is incredible. To the senior leaders and the Leads for the CSDA project it has never been about buying the newest and coolest things only to have them become obsolete before they are fielded to the Soldiers who need them the most. The CSDA project is more about leveraging industry solutions and creating the potential for placing the most advanced, affordable solution in the hands of our Soldiers from a system perspective. Considerations for the complete system include the devices, Apps, information security, backend servers and software, power management, transport layer solutions, life-cycle sustainment. The project also continues to assess even such mundane things like how to use Smartphones without the Soldier having to remove their

A Soldier uses his Smartphone to track the friendly forces at the Network Integration Evaluation 12.2.

gloves to use the touch screens.

As the project matures, the most frequent question asked by industry partners, users and interested partners continues to be: "Has the Army selected a phone and an operating system?" The short answer is, no! By remaining true to this approach the Army retains flexibility to look across many industry partners and avoid costly solutions that must be sustained indefinitely. This approach also provides the opportunity to stay current with new and emerging technologies over time.

Early in the discovery phase of the project, the CSDA leads attended a conference that focused on developing a tactical Smartphone. The goal was to deliver a rugged device that weighed in at no more than 3.5 pounds, used the Android 2.0 operating system, cost no more than $5,000 per device, and could be developed and delivered in less than 5 to 7 years. The CSDA project leadership agreed this was not the right solution. The Soldiers needed a low-cost solution that could be easily replaced if damaged or upgraded/replaced when better technologies became available.

Applications or "Apps" are an important and essential element of the project. Using the model developed in the commercial side of the market, Army leaders embarked on several efforts to address the challenges of providing solutions for Soldiers.

CSDA identified three probable sources for Apps as well as how to get Apps into the hands of Soldiers. Industry anticipated Army managers would come to their doors with an open checkbook (as traditionally occurred) to have expensive software crafted at great expense and time. In keeping with the Agile Process model, the CSDA project endeavored to find low-cost solutions to address app requirements they could not build for themselves.

The Signal Center of Excellence took on the challenge of training individuals how to write and build apps. The intent of the course was to take individuals within the Functional Area 53 (Information Systems Management) and give them the skills and tools to write Apps in order to meet the immediate needs of the commands the FA 53 officers are assigned to. Over time the course was opened up to allow others to attend and receive the same skills. As part of the training individuals build actual apps that are available for both Android and Apple devices.

The third source for apps identified by the CSDA project is from the users themselves. The Army hosted the "Apps for Army" competition to see if this was a viable source for Apps – the response of this competition far exceeded expectations. At Fort Bliss, the BMC staff generated more than 85 tactical and operational Apps used during the evaluation and assessment of various technologies and solutions provided from industry. Additionally a number of Apps were created by the Soldiers from 2nd Brigade, 1st Armored Division – the brigade combat team dedicated to conduct the Army's Network Integration Evaluation. Several Apps were written by Soldiers while they were in the field conducting the NIE.

To ensure the apps available to the Soldiers are safe and secure, policies and protocols have been implemented to review the source code of all Apps designed for Smartphone and device use. The review has three primary goals: (1) a legal review to ensure copy write laws are not violated; (2) a technical review to ensure that the technical code does not contain harmful code or generate data to third-party sources (as most commercial Apps do); and (3) a doctrinal review by the proponent school or center of excellence. The CIO/G6 created a "Store Front" as a repository for apps that meet these prescribed standards. As the

(Continued on page 10)

(Continued from page 9)

Army Store Front comes on line, there will also be a feedback mechanism for apps-users to provide evaluations, similar to the feedback mechanisms used in commercial apps stores.

Nothing is ever as simple as it appears. Because of the potential for Soldiers to use Smartphone technologies in operational combat environments, it is absolutely essential the technologies and applications meet the established standards for protecting sources and users of data and information. Data must be protected while at rest, in transit, and in-process. This also requires that devices and operators be able to operate at various levels of security and have the ability to move back and forth without having separate devices. During the early phases of the project, hardware requirements to operate above secret level were not achievable with commercial devices while maintaining affordability.

An initial challenge was overcoming institutional and cultural traditions. Many of the policies and procedures in use throughout the government are residual Cold-War era approaches established to allow for zero-risk. Time and the environment have changed – the threats and technologies of the Cold-War have changed or no longer exist.

SSG Gilbert Hinojosa of 2BCT, 1st AD using his Soldier Warrior ensemble Smartphone during operations at the Network Integration Evaluation 12.2 at Fort Bliss, Texas.

Similar to commanders of the past, commanders in today's operating environment at all levels must manage risk to minimize adverse impacts on their operations and their Soldiers. By connecting Soldiers to the network, we have opportunities to provide Soldiers the ability to access information at the edge, and to take advantage of Smartphone technologies against their opponents.

Although the process of achieving the Information Assurance measures necessary to meet the intent of the project have not moved as quickly as one would like, the good news is they are moving in the right direction and gaining traction throughout the IA community.

Initially TRADOC approved eight Pilot projects to assess the value and utility of using Smartphone technology.

Seven of the pilots focused on the institutional Army, primarily in the training base. The projects were developed by the proponent schools and ranged from advanced individual training to Officer Advanced Leadership Courses. Portions of our schools programs of instruction were converted into digital media on a variety of devices ranging from iPods, readers, tablets and phones. The eighth pilot focused on the tactical and operational uses of Smartphones. In each case, the results of the pilots far exceeded expectations.

As the CSDA leads reviewed and analyzed the results of the Pilot projects a dramatic trend emerged. Graduation scores of the Soldiers using CSDA technologies increased an average of 10% across the board over the scores of their peers. In one case, a self-paced class graduated from advanced individual training, two weeks sooner than average class graduation times. As the trends continued to emerge, the CSDA team began to look at the "why" in an effort to isolate to root cause for the dramatic improvements of the Soldier's scores.

In several cases Soldiers attributed using e-readers to access publications outside the classroom that previously they were unable to take back to the barracks due to high printing costs; this access gave them an incentive to continue studying after the normal duty day.

It was also identified the Soldiers were in many cases using the technology in their off-duty time to compete against other Soldiers, for better, faster, and more accurate results using their interactive learning modules.

Training became fun. The Soldiers provided critical feedback that indicated they expect to have the same quality products found in the commercial market, and were quick to identify production flaws.

The selection of the Brigade Modernization Command at Fort Bliss, to participate in the CSDA project is an additional benefit. The mission of the BMC is to conduct physical integration and evaluation of the

network, capability packages and other core capabilities in order to provide Doctrine, Organization, Training, Materiel, Leadership and Education, Personnel and Facilities recommendations to the Army as part of the Brigade Modernization Program – in short, to evaluate and assess solutions being considered for the modernization of the brigade combat teams across the force.

Given a fully functional BCT (2/1 AD) coupled with the large training areas and airspace of Fort Bliss and White Sands Missile Range -- unmatched at any installation -- and wide use of the available electromagnetic spectrum, the right environment for evaluating Smartphone technologies under realistic operational conditions results.

BMC conducts two major evaluation events per year in partnership with the Army's Test and Evaluation Command, and the ASA-ALT's Systems of Systems Integration Office Directorate. Additionally, small targeted excursion events are conducted in conjunction with other 2/1 AD training events.

The Network Integration Evaluations are formally structured and instrumented activities designed for an in-depth look at how technologies work in the hands of the Soldiers. In addition to formal data collection and analysis, Soldiers are given the opportunity to provide their unstructured and subjective feedback on how the technology and solutions worked and what utility and value it provides – in essence, the 2/1 Soldiers become the ultimate advocates for our deployed or deploying combat formations.

The CSDA project has used the NIE to evaluate the full spectrum of solutions with great success. It continues to inform the CSDA management on what paths to pursue, and not pursue. Technologies that look good on paper or in the lab turn out to not provide value-added to the Soldiers when the ambient temperatures exceed 117 degrees. Other technologies have performed exceptionally well and are potential game changers.

As a direct result of the work at the BMC, the Soldiers of 2/1 AD and many others, a number of solutions have already made it into the hands of Soldiers deployed around the globe and in combat operations in both Afghanistan and Iraq.

The CSDA project has informed the Army on the viability and military utility of using Smartphones across a full spectrum of military operations and domains with great results. Numerous Programs of Record are examining the incorporation and integration of a wide range of technologies into their efforts. The technologies have proven to be battle-worthy and durable, low cost solutions for fundamentally changing how Soldiers communicate and learn. The sister services are now looking at how these technologies can serve them and their Sailors, Airmen and Marines. The ground-swell continues now as the rest of government begins looking at using the same technologies across a full spectrum of missions and task. Smartphones are no longer the purview of senior leaders and executives, but have become a critical tool for everyone and show great promise for connecting Soldiers to the Network and empowering our Soldiers at the edge.

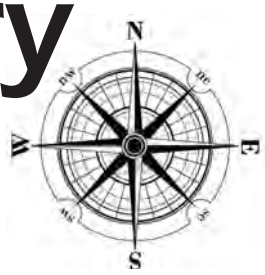
BG Randal Dragon ***currently serves as the commanding general, Brigade Modernization Command at Fort Bliss, Texas. Commissioned as an Infantry Officer, BG Dragon has over 32 years of service including numerous deployments to Macedonia, Kosovo, and Iraq. Prior to his current assignment BG Dragon served as the deputy commanding general for the 1st Infantry Division in Iraq. BG Dragon also commanded the operation group at the National Training Center at Fort Irwin, Calif.***

Mike McCarthy ***currently serves as the director of operations for the Brigade Modernization Command Mission Command Complex at Fort Bliss, Texas. For the past two years he has served as co-lead for the U.S. Army's "Connecting Soldiers to Digital Applications" project. Mr. McCarthy has spent the past 17 years in various positions training Soldiers with modeling and simulations.***

Acronym QuickScan

AD – Armored Division
AIT – Advanced Individual Training
ARCIC – Army Capabilities Integration Center
ASA-ALT – Assistant Secretary of the Army for Acquisition, Logistics and Technology
BCT – Brigade Combat Team
BMC – Brigade Modernization Command
CIO – Chief Information Officer
CSDA – Connecting Soldiers to Digital Applications
DOTMLPF – Doctrine, Organization, Training, Materiel, Leadership and Education, Personnel and Facilities
FA – Functional Area
IA – Information Assurance
NIE – Network Integration Evaluation
SOSI – Systems of Systems Integration
TRADOC – U. S. Army Training and Doctrine Command

The Future of Military Mobile Computing



By COL Bruce Caulkins

Significant and enduring are two words that reflect the reality we face today regarding mobile computing technologies.

The ubiquity of smart phones, tablets, and other mobile computing devices in the commercial world makes cellular technologies a must for the future military network to support. The wide use of Smartphones also ensures that any potential users – especially those military users who are under the age of 30 – are more comfortable with the technology and therefore easier to train and understand how to use this new technology on the battlefield.

Currently, these technologies' vulnerabilities prevent us from using most of these devices for official work. Cyber vulnerabilities exist that do not yet allow the military to fully use smart phone technology on the military network, or Global Information Grid. Common Access Cards, Federal Information Processing Standard 140-2 certifications, and software compliance are just a few of the hurdles that we need to overcome to make cellular technology a reality.

Cultural bias is also an issue. Everywhere in the federal government, you can talk to the leaders and engineers in any agency and they will tell you that they are excited about this technology and that they will support any action to get smart phones and apps onto our networks. Then, you can walk down the hall in that same agency and the security folks will tell you that they can't see smart phone deployment happening any time soon, if at all. While the security professionals certainly have a legitimate point, "just saying no" is not a viable course of action any longer. Too many leaders and Soldiers are demanding this capability in garrison and on the battlefield. So we need to continue moving forward.

Last year, the Signal Center of Excellence published a cellular vision paper for the Army that outlines future steps the Army must make to move forward in this area. The paper can be downloaded at http://www.ecrow.org/pdf/Army_Cellular_Capability_Development_Strategy_16_August_2011.pdf. In that document, we proposed an integrated strategy that will give the Army the following capabilities:

- Ensure an effective, cost saving expenditure of resources, while eliminating redundancies and developing a solution that meets Warfighter needs
- Develop dynamic, secure smart phone software applications to provide ease of use and enhancements to Soldier use of handhelds or tablets
- Connect the mobile and dismounted Soldier to the network through an integrated solution
- Develop cellular technologies that can deliver high throughput at a low cost in a scalable, easy to deploy, easy to operate network architecture
- Exploit emerging cellular/broadband technologies and leverage commercial communications infrastructure for units both in garrison

(U.S. Army photo)

Soldiers utilize Distributed Common Ground System-Army, or DCGS-A, operations center at Aberdeen Proving Ground, Md. U.S. Army Research, Development and Engineering Command's communications-electronics center's Intelligence and Information Warfare Directorate hosts the Tactical Cloud Integration Lab in an effort to expedite cloud computing technologies to the Soldier.

(Photo by SSG Joshua Ford)

LTC Mark Stiner *(left)*, program manager for the Joint Tactical Radio System Handheld, Manpack and Small Form Fit, shows GEN Peter W. Chiarelli, the Army vice chief of staff, how to operate part of the JTRS during a training event with Paratroopers from Company C, 1st Battalion, 505th Parachute Infantry Regiment, 3rd Brigade Combat Team, 82nd Airborne Division, at Fort Bragg 3 March.

and while operationally deployed
•Initiate phased insertion of commercial wireless technologies, interoperable with tactical networks, and complementary to programs of record, with legs to future (WIN-T, JBC-P, Nett Warrior, and JTRS)
•Implement an Army unified communications strategy, designed to enhance garrison/mobile networks through efficiencies in delivery and routing of voice, video, data through network convergence.

These seven imperatives plot the way for the future. While recognizing the cyber vulnerability issues, they also show that inserting various commercial wireless and cellular technologies into specific programs of record will allow mobile computing technologies to flourish and support those various programs of record's missions.

To accelerate these and other advanced communication capabilities into the force, the Army has created the Network Integration Evaluation at Fort Bliss, Texas. The NIE exercises are conducted twice per year and are designed to integrate and dramatically advance the Army's tactical network. To do so, the Army's Brigade Modernization Command, in conjunction with the Army Test and Evaluation Command and Systems of Systems Integration Directorate, accomplishes the NIE exercises in order to conduct integrated and parallel Operational Tests of select Army programs of record. Further, the BMC and its partners use the NIE to evaluate development and emerging network capabilities in an operational environment and to assess non-networked capabilities in an integrated operational environment.

From the outset, the NIE has been a vital player in assessing mobile computing capabilities, both within programs of record-type systems and within standalone systems under evaluation. These future mobile computing capabilities will allow the Army to better support the needs of the commander all the way down to the individual Soldier, whether in garrison or in an operational environment.

COL Bruce Caulkins, ***Ph.D. is the G6 for the Signal Center of Excellence at Fort Gordon, Ga. He is a Signal Corps Functional Area 53 Information Systems Management officer and has recently served as the chief of the Accelerated Capabilities Division, the commandant for the Leader College for Information Technology, and the director of the School of Information Technology. He has written numerous articles in the cyber and cellular areas and his doctorate is in Modeling and Simulation, focusing on network security.***

Acronym QuickScan

ATEC – Army Test and Evaluation Command
BMC – Brigade Modernization Command
CAC – Common Access Card
FIPS – Federal Information Processing Standard
GIG – Global Information Grid
JBC-P – Joint Battle Command – Platform
JTRS – Joint Tactical Radio System
NIE – Network Integration Evaluation
SIGCoE – Signal Center of Excellence
SoSI – Systems of Systems Itegration

Delivering Training to the Point of Need

By LTC James T. McGhee

During the past few years there has been a worldwide explosion in the sale and use of mobile electronic devices such as "smart" phones and tablets. An entire generation of learners is becoming as familiar with the iPad as they are with a television.

Leaders at academic institutions throughout the world are touting the value of these devices in enhancing student learning experiences However; educators will most likely not be able to assess the full value of these new technologies for many years. The speed at which industry is able to develop and manufacture increasingly powerful devices makes it difficult to keep up with the educational benefits of the latest mobile capabilities.

Army leaders, through the Connecting Soldiers with Digital Applications initiative, are exploring the value of these devices in order to support the visions outlined in the Army Learning Model and Doctrine 2015 to provide Soldiers with Army information, doctrine, and training and leader development content at the point of need. Two years of continuous concept exploration through various pilot programs at Army Centers of Excellence have clearly demonstrated value in delivering Army information, along with training and leader development content, to Soldiers through mobile electronic devices.

Far too often, the discussion about the military use of mobile electronic devices turns to Information Assurance and the inability to connect commercial mobile devices to the Department of Defense Networks. The security risks associated with mobile devices are real. According to a Global Study on Mobility Risks, 51% of businesses surveyed lost data last year due to employee use of mobile devices. The Department of Army Chief Information Officer takes these threats very seriously, but is also looking for a solution that will provide the Army with a "secure" mobile device(s) similar to its current use of the RIM Blackberry. Whether a solution is announced this year or next, it is unlikely that the Army, given current resource constraints, will be able to purchase enough devices to issue an approved device in great quantities to the field.

There is no need for the Army or its institutions of learning to wait for a secure mobile solution. According to recent Army study conducted by the TRADOC Analysis Center at select Army Centers of Excellence, the number of Soldiers attending Army schools who own a personal mobile device exceeds 75%. It's the "Bring Your Own Device" solution that will enable the Army to move forward with the development and delivery of unclassified Army publications, doctrine, and training content at the point of need. It's all about the content. The truth is the majority of the Army's doctrine and training content is unclassified and approved for public release. While the Army waits for a secure solution that will allow a secure mobile device solution to access DoD net-

(Photo courtesy of General Dynamics)

A student uses a Smartphone to learn about the capabilities of the Satellite Transportable Trailer.

(Photo courtesy of General Dynamics)

An instructor uses a tablet device to facilitate discussion in his class.

works, it has enough unclassified material available to convert to mobile formats to keep doctrine writers and training developers employed for months if not years.

What Army learning institutions can do today is train its personnel to format doctrine and training content for mobile devices. For example, outdated PDF files continue as the Army standard for mobile delivery of publications but their use on most mobile devices does not provide a user friendly experience. The industry standard format for most mobile devices is the ePUB. The ePUB and Apple's new revolutionary iBook are both outstanding formats that can deliver a positive user experience that enhances and sustains learning at the point of need. Along with outdated formats, the Army continues to follow outdated publishing directives tied to traditional paper printing requirements. Through mobile delivery, the content developer is no longer constrained by archaic rules, such as the requirement for all photos, maps, and charts to be delivered in grey scale to avoid the excessive costs associated with color printing. Content and training developers should be moving forward to develop their skills, learn the process and begin formatting all of their unclassified material as ePUBs. TRADOC is moving forward to establish an ePUB policy along with a public accessible Central Army Registry and supporting Apple and Google Apps to distribute ePUB files to personally owned mobile devices. The mobile revolution of content delivery is upon us and those who choose not to move forward rapidly are doomed to fall behind. For more information on CSDA, formatting content for use on mobile devices, or delivery of content through mobile apps, contact the Mission Command Center of Excellence's CSDA point of contact, LTC James T. McGhee at 913-684-6356, or james.mcghee1@us.army.mil.

LTC James Todd McGhee ***is a Simulations Operations Officer assigned to the Mission Command Center of Excellence at Fort Leavenworth, Kan. He currently serves as the U.S. Army Training and Doctrine Command's lead action officer for the Connecting Soldiers to Digital Applications initiative and serves as the TRADOC voice to organizations outside of TRADOC to help define mobile requirements to meet the needs of the Soldiers.***

Join the Discussion
https://signallink.army.mil

Acronym QuickScan

CIO/G6 – Department of the Army Communications Officer
CSDA - Connecting Soldiers with Digital Applications
DoD – Department of Defense
IA – Information Assurance
TRAC – U. S. Army Training and Doctrine Command Analysis Center
TRADOC – U.S. Army Training and Doctrine Command

Mobile training devices fully integrated into classroom training

By Al Makowsky

Mobile computing devices are fully integrated into Signal training, producing huge savings and making training more accessible and individualized.

The General Dynamics LandWarNet School has been continually changing its training content to keep up with the pace of change. Less than 10 years ago, the LWNS trained Soldiers in the traditional way using PowerPoint slides in a classroom lecture format, and giving Soldiers large binders of printed material as take home reference for their courses. With the introduction of the Joint Network Node into the tactical network in the mid-2000's, the school needed to produce training content that was able to be updated quickly and distributed to Soldiers easily.

To do this, the LWNS converted all its training material to be Adobe Flash-based. This gave the content more flexibility through the use of animations and better graphics to depict equipment. Conversion to Flash also reduced the overall file size of presentations, allowing the training content for any particular course to easily fit on a single DVD. Taking up less space for the lesson presentations also allowed the school to put a vast library of COTS and Technical Manuals, and other reference materials on the DVD.

(Photo by Bonnie Heater)

PFC Jonathan Fancher, a 25Q, multichannel transmission systems operator-maintainer, uses the Motorola Zoom Android based tablet to read the Quick Response Code, on the AN/TSC-185 STT.

The result is known as an Electronic Quick Reference Guide or EQRG. Digital training content allows for quick update and putting it on a DVD allows for easy distribution to the Soldiers. Printing costs were also a factor at this time and the movement to digital training material has virtually eliminated the need to provide printed content to the Soldiers. This alone saves almost $2 million a year that is reinvested into providing additional training capabilities at the LWNS.

Today, the advent of tablet computing and Smartphone technology has forced the school to once again change with the times to provide a better training capability. Flash-based products do not play well on many of the different hand-held devices that are out there.

The Army Learning Model encourages training to be available to the learner at the point of need. That demands mobile content that is accessible and playable on any platform the learner may be using. To meet these demands, the LWNS is repurposing its training content to be based in HTML and able to be used on any platform that has a browser.

Students at the LWNS can access any training content throughout our Brant Hall facility at the point of need. Whether they are in a multimedia classroom, using a 3D equipment simulation, or working on the actual equipment, they can access training material from which to learn.

Content not only consists of classroom presentations, but also includes more PC-based simulations, CBTs, and "How To" videos. Away from the school, they can access this same training content by going to the SIGCoE's LandWarNet eUniversity. And, yes, they continue to get the EQRG for their class on a DVD. The LWNS evolution in training content has been a conscious effort to provide flexible learning tools in a format that makes them available to the Soldier learner at the time and place he/she has a need to learn.

Al Makowsky ***is a retired FA53 officer. He is currently the Training Operations Manager at the General Dynamics LandWarNet School at Fort Gordon, Ga. His team of training developers and multimedia technicians are using mobile computing technology and creating mobile training content to support implementing the Army Learning Model at the Signal Center of Excellence.***

Pilot program evaluating personal tablet device use across campus

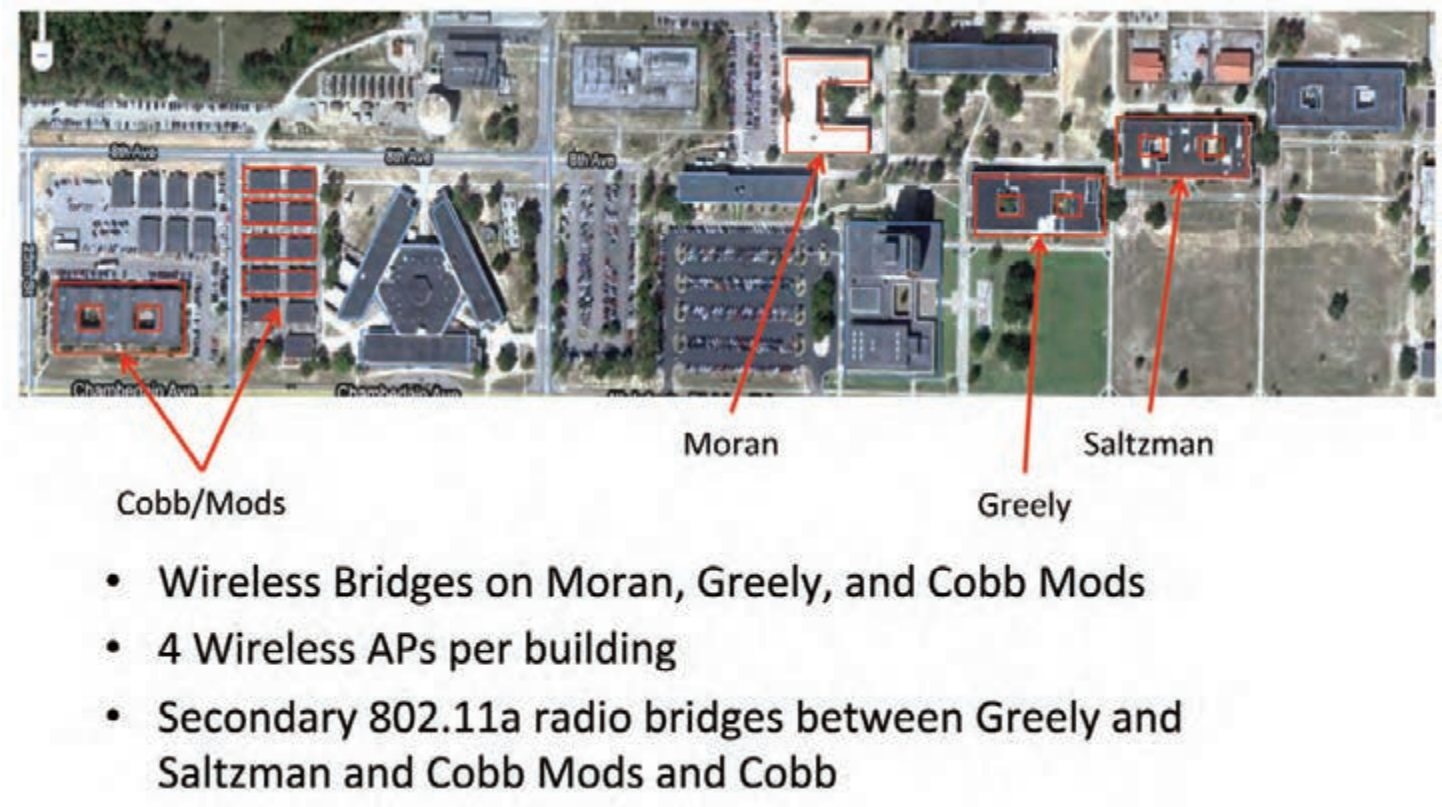
By LTC Gregory Motes and CPT Chris Braunstein

After the introduction of Apple's iPad in 2010, there was natural interest among leaders of the Army's education system to evaluate the potential of tablets running Smartphone operating systems for training support in military classrooms. With Soldiers' ongoing development of mobile applications at Fort Gordon, MG Alan R. Lynn, commanding general and Mr. Joe Capps, then deputy to the commanding general of the Signal Center of Excellence, worked in collaboration with MG Mark Bowman from the Army CIO/G6 to acquire 150 tablet devices for the SIGCoE's mobile computing pilot program. An additional 150 tablets were acquired for the parallel pilot program at the U. S. Military Academy. Both programs were given the restriction that the devices would not connect to the Non-secure Internet Protocol Router Network.

The prevalent belief at the time was that the inclusion of tablets with access to relevant information deemed useful for the students could increase performance in the classroom. With this, the SIGCoE formally created a pilot program called the SIGCoE Connected Personal Tablet pilot, which determined several areas useful for exploration, identifying three separate focus areas: academic administration, student socialization, and institutional learning.

Academic administration goals included determining how to use connected personal tablets for the students to send and receive information about pending or recent events, while providing a gateway of communication between the students and their class leaders, small group leaders, instructors and course adminis-

(Continued on page 18)



This graphic shows the U. S. Army Signal Center of Excellence Connected Personal Tablet network layout on the Fort Gordon academic footprint.

(Continued from page 17)

trators. An example of this included using a calendar program on the device to allow administrators and leaders to note upcoming events and locations/uniforms that the students need to be aware of, and to allowing instant access to a flowing schedule. There was also interest in connecting the students to Blackboard for ubiquitous access to classroom resources already provided to the students.

Student socialization goals included using the devices to connect the students to each other and to the larger community using social networking tools and norms. Among these are connections to MilBook and MilWiki, as well as social networking sites like FaceBook and Twitter. During the pilot program, multiple resources that the students could access switched from AKO username / password authentication to using CAC/PKI for authentication, which lessened the usefulness of the tablets and highlighted a significant challenge to mass adoption of new devices given the legitimate security concerns provided by untested and unintegrated devices.

Learning goals included examining course content that can be used for preparation, augmentation, replacement, refreshing and assessment. Preparation material includes any read-ahead material or courseware that instructors might require as a prerequisite to instruction. Currently a vast amount of content resides within Blackboard, and the SCPT intended to examine the ease and utility of converting that to a means that is acceptable on a tablet. Augmentation includes having material and tools that students can use as part of their normal coursework to increase their time to acquire the learning objectives. As an example, having an app that can be used to augment instruction on subnetting could be useful to students attempting to learn the complexities of that subject. Additionally, having the ability to use a tablet to port into a Cisco Switch, or to connect remotely to a server for management, can augment the instruction. Replacement is simply looking at courses and instruction that can be suited for distributed learning on a tablet allowing students to learn those topics without having to come to class.

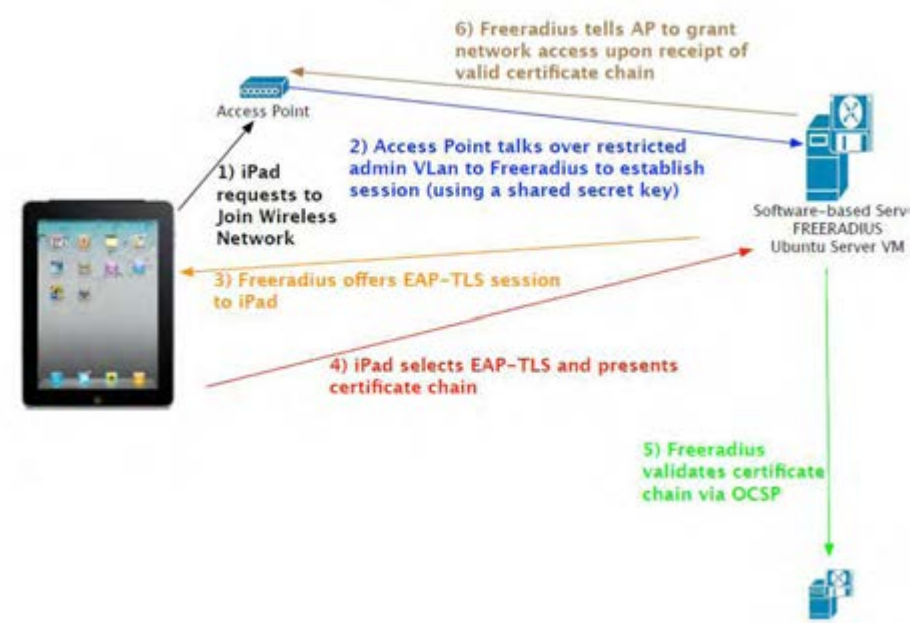
As the Army moves toward the goals of the Army Learning Model 2015, identifying courses and material that can be supplanted by digital device instruction is an area requiring exploration. Refreshing material is designed for alumni of a particular course to go back and review information from their studies to inform them in certain aspects of a problem. An example of that within the SIGCoE's context could be the eventual creation of course material from our Basic Officer Leadership Course and then to make that material available to students coming to SCCC as a refresher. Furthermore, as an increasing amount of content is available on personal devices, once a student graduates from a course, they should have alumni access to that information if they need to recall it during their current duty assignment.

The fifth dimension here is supported using tablets and apps to assess "Assessing Students." In addition to formal assessment, computer based training modules already in existence have shown numerous ways to provide checks on learning and self-assessment. With the data that can be collected across a wide range of apps, a depth of assessment tools and techniques can be applied to understand the student's learning styles and adapt the material based on their preferences. As an example, some students find videos favorable to detailed text, while others prefer to read the technical details in depth in order to grasp complex subjects.

Apps

One identified challenge with many of the pilot programs that are examining mobile devices is their lack of specific applications that can be provided to the early adopters. With the SCPT, students were provided with access to several commercial applications that could be used for classroom and office productivity, including applications to create new documents, spreadsheets and presentations, as well as apps that can assist in managing notes. Furthermore, they were encouraged to download additional free apps to provide feedback on the capabilities of those apps in relationship to professional military education. The users were informed that information they stored on the device not violate military regulations in terms of storing Personally Identifiable Information and meeting Data at Rest requirements. Furthermore, they were cautioned against creating or accessing information that was deemed For Official Use Only due to security concerns and the lack of a current Security Technical Implementation Guideline for the tablet.

Additionally, previous apps created by the SIGCoE were installed, including apps for Physical Readiness Training and Army Values. The SIGCoE also discussed the creation of a number of additional apps, including a Decision Matrix app, QR Code trainer, Signal Connect, and an app for Generator Power Distribution. Furthermore, the use of virtualized desktops that the tablets could access through VMware's View technology was presented as an option to allow the students to connect to complex Windows based applications like the unclassified training version of the Command Post of the Future or Network Monitor programs like SolarWinds.



Here is an illustration of the network authentication signal flow that occurs when joining the network.

Technology Management

Moving toward mixing public and custom apps created some interesting management problems addressed in the SCPT. On any of the current mobile operating systems, downloading apps from a public market required that the device use unique login accounts. Inclusion of the iPad as one of the tablets tested also meant that we had to individually activate the device through iTunes and manually load the apps to the devices.

As discussed below, the technology for "imaging" devices matured during the course of our 15 month pilot. This eased some of the technology management hurdles for iOS devices. At the beginning of the effort, though, individual iTunes accounts were created for each of the students and tied to a domain email address provided by the SIGCoE. This allowed the legal transfer of applications purchased for "Student 1" to stay with the tablet as it was reassigned to future classes. Subsequently, bulk purchasing of applications has also made it easier for a school to volume license applications for legal inclusion onto school owned devices.

A further goal of the SCPT was to examine the procedures and technical infrastructure required to support the program. Configuration management was a big challenge because many management tools were in their infancy or did not exist. Early on we had to wipe, update, and prepare each individual tablet one at a time in an assembly line type operation. This was further complicated by the fact that the tablets required a USB connection to a computer in order to activate prior to use. We initially had a bank of laptops with iTunes installed that students would use during the initial issue process. A new operating system update fixed this problem and students were able to complete the tablet setup process without connecting to a computer.

Our final issue process was to issue the tablets and accessories, require students to read and to sign the Acceptable Use Policy and hand receipt, to connect their tablets to a "bootstrap" network that would only allow them to connect to a web server to download a configuration profile, and to finally download an application to complete a survey and proficiency test. This process initially took two hours per group of 20 students, and was eventually reduced to approximately 45 minutes depending on how many questions students had.

Even though we came up with a pretty manageable process for issue and turn-in of tablets, we were still faced with additional problems. It was cumbersome to keep whatever tablets we had in our inventory updated to the latest operating system due to having to plug each one into a computer for updates.

We were also concerned about students' personal information persisting between updates, requiring a manual inspection of each tablet to ensure that students were wiping them as instructed during turn-in. Keeping a class worth of tablets charged for the next issue required multiple power strips and power outlets.

Eventually we acquired a cart with storage shelves for 30 tablets with 30-pin dock connectors for each device that solved all of these issues. The cart was mobile and had a standard power cord that would keep the tablets charged while in storage. A single USB cable connected to a computer allowing for the wiping, updating, and configuration of all 30 tablets in the cart. An application called "Configurator" allowed us to wipe all the tablets, update them to the latest operating system, and push apps (both enterprise and from the iTunes store) and configuration settings to each device simultaneously.

Many of the goals of the SCPT required Internet functionality. There was value in examining the effects and management challenges of mobile devices on a Local Area Network.

Leaders at the SIGCoE quickly determined that a 100% com-

(Continued on page 20)

(Continued from page 19)

mercial network would be. required and set out to build a cheap and reliable testing ground for the students, acquiring a standard commercial cable internet connection that provided 25 Mbps down / 3 Mbps up of bandwidth. We constructed a wireless repeater network using 802.11g access points and bridges.

The bridges were installed on the top of buildings and the access points were wired using CAT 5e cable. All of the equipment was powered using Power over Ethernet switches. Since we only were supporting 150 devices and a relatively small footprint we decided to keep everything in the same private subnet, allowing us to keep the wireless equipment in the Data Link layer (Layer 2) of the Open Systems Interconnect model. Because of this we did not have to install routers in each building that vastly reduced the cost and management requirements of the network. Despite this being an "open" Internet connection, we still were required to maintain as much adherence to Army Information Assurance Regulations as possible (AR 25-1 and 25-2). We installed a firewall at the perimeter of the network that blocked all non-web services.

Initially we were concerned that this would cause problems with applications that the students were downloading, but we discovered that almost all apps use web ports and protocols for data transfer. This could be a general trend, or just a reflection of our small user base. A transparent open source web proxy was also installed to block access to restricted material (pornography, gambling, hacking, etc.) and for auditing purposes. All web traffic was redirected from the edge router to the web proxy server using the Web Cache Communication Protocol. The redirected web traffic was also cached locally in an attempt to reduce bandwidth usage of the Internet connection.

A method was needed to ensure that only SIGCoE issued tablets were authorized to connect to our commercial wireless network. This would ensure that only authorized students were connecting as well as reducing the bandwidth needs and monitoring requirements. There are currently no known viruses/malware on the iOS platform (other than on jailbroken devices - which was not possible for the iPad 2 with the version of the operating system that we were using). By limiting the network to only SIGCoE issued tablets we could greatly reduce the risk of a virus or other rogue element causing data leakage or other destructive behaviors on the network. Most non-enterprise wireless networks use a pre-shared key for access control or are open access. Using a pre-shared key would have been problematic for us. We would not be able to ensure that students didn't share the password with other individuals and would have to constantly monitor the network for rogue devices. After a class turned in their equipment we would have to cycle the key on every access point, which would have been time consuming and pointless. We needed to use an enterprise class authentication system that was not based on credentials. Based on this fact we designed a certificate based authentication system that ensured only SIGCoE issued iPads that were signed out to a student would be authorized on the network.

The SIGCoE had already built a virtualization cluster for hosting code repositories and other development tools, so we had plenty of server space for this solution. The first step was to stand up a Remote Authentication Dial In User Service server. RADIUS is a client/server protocol that can be used to authenticate users or devices before granting them access to a network. This server would act as the "gatekeeper" to our network, only allowing devices with valid certificates onto the network. When a device attempts to connect to a wireless access point a connection is established between the access point and the RADIUS server over an administrative Virtual Local Area Network to establish a session using a shared secret key.

Next, the RADIUS server offers an Extensible Authentication Protocol - Transport Layer Security session which is established between the tablet and the RADIUS server. This session is unique because the tablet is not assigned an Internet Protocol address at this point ensuring that it can only communicate with the RADIUS server and not other devices on the network or the internet. The tablet presents the digital certificate chain to the RADIUS server over the encrypted tunnel. Finally, the RADIUS server uses the Online Certificate Status Protocol to validate the certificate chain and either approves or disapproves network access.

We also needed a way to generate the digital certificates in an automated process that could also be controlled by the SIGCoE during the tablet issue process. We created a Simple Certificate Enrollment Protocol server that could issue and revoke digital certificates. The iOS operating system includes support for SCEP, OCSP, RADIUS, and EAP-TLS. Additionally, all of these protocols can be configured using a "configuration profile" which is an Extensible Markup Language file that allows for the distribution of configuration information to iOS devices. These profiles can be installed on a device over a USB connection, by sending it to a device via e-mail or a website hyperlink, or through a Mobile Device Management solution that would push profiles to devices over the air. We generated a configuration profile for each class issue which included the SCEP enrollment request, the Wi-Fi network SSID settings, and two self-signed digital certificates to ensure the validity of the servers that the tablets would authenticate with to

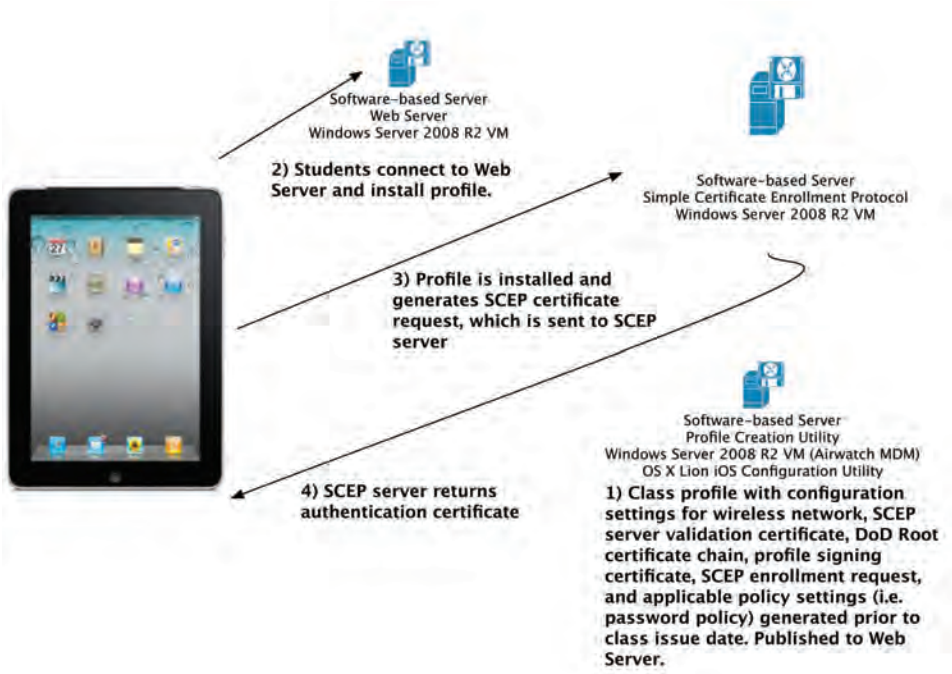
protect against man-in-the-middle-attacks. This configuration profile was also digitally signed to protect against tampering with the profile and so that tablets could verify its authenticity.

This system had additional control measures built-in. We would only allow the SCEP server to issue certificates during the issue process, which ensured that rogue tablets could not get a certificate during non-issue times.

The SCEP certificate issue process and configuration profile download were restricted to the "bootstrap" network that only connected to the web server hosting the configuration profile, ensuring that tablets would only be able to be provisioned during controlled issue. We could disable the "bootstrap" network when it was not in use, ensuring that attackers would not be able to maliciously attempt to get the configuration profile or digital certificate chain.

A configuration profile could not be extracted from an iOS tablet, ensuring that users could not transfer their certificates to another device. A user could remove the configuration profile by connecting the device to a laptop via USB and restoring the operating system, but this would permanently remove the profile which would mean that their device would not be allowed onto the network. A configuration profile could also configure further restrictions such as stopping the camera from working or removing access to the iTunes market - almost all of the iOS configuration settings and features could be controlled. Using this method we could tie network access to our Acceptable Use Policy, ensuring that devices conformed to our policy before being allowed to connect to the network. We could also revoke the certificate on the SCEP server for a particular device, allowing us to remove individual devices from the network.

This system would also work on Android based devices, however extra care would have to be taken due to the fact that the Android operating system does not use a "configuration profile" system for device management.



Initial provisioning process for an iPad with certificate authentication.

The digital certificate could be stored in an encrypted form using a Public Key Infrastructure token such as a Common Access Card on the device SD Card or internal storage. CAC card readers are available for purchase today, although they are expensive and the software has not matured enough for exclusive day to day use.

We performed a limited amount of testing of Android tablets but never implemented an Android compatible version of this solution.

In addition to the servers required for the network authentication system, we used an open source network monitoring solution called Zenoss. We installed Zenoss as a virtualized application that was managed from a web console. Using Zenoss we could monitor all aspects of the network through polling (pinging devices on the network to check their status) as well as through the Simple Network Management Protocol.

SNMP exposes management data in the form of variables on the managed systems, which describe system configuration and state. A managed device runs an "agent" that can send asynchronous notifications called "traps" to the management platform containing data such as CPU usage, temperatures, bandwidth utilization, etc. An agent can also be polled through a "GetRequest" that will return the status of desired variables. All variables are defined by management information bases which describe the nature of a device subsystem.

Overall, the tablets presented a moderate management load to the network. Traditional network monitoring must still be performed (link status, service availability, etc). We had reduced the concern for malware and viruses significantly, but still had to maintain active monitoring of the servers. An intrusion detection system would have increased the likelihood of detecting an attack on the network, although we did not install one

(Continued on page 22)

(Continued from page 21)

because we did not have the necessary manpower to fine tune and monitor it. An average of one or two tablets were broken per class during the course of the pilot. Technical support requests were much lower than if using desktop or laptop based systems, averaging less than one support request per class. Additional challenges arose such as wireless access point coverage, bridge link alignment, and ISP outages that added to the management tasks.

Classes

During the initial planning for the SCPT, we discussed issuing devices to multiple different courses at the Signal Center, including the Signal Captains' Career Course, the Functional Area 53 Information Systems Manager Qualification Course, as well as consideration for the Warrant Officer classes.

Ultimately, it was decided that the best effort was to focus on a single course and try to establish continuity over time with the instructors, small group leaders and training developers. Of the groups invited to the initial planning meetings, the SCCC course leaders were the most enthusiastic about participating in the SCPT, so the decision was made to issue them the devices.

Each SCCC has 40 students and 2 small group leaders assigned, so 42 devices were set aside for each of 3 courses, with remaining devices available to the application developers and a limited number of instructors and cadre.

Data Collection Metrics

Early on, it was predicted that success for this pilot hinged on the willingness of the cadre to explore the utility of the devices, as well as ensuring that the technology did not disrupt the course programmed instruction. Additionally, it was determined that the inclusion of the Army Research Institute for Behavioral and Social Science could provide a resource for analyzing whether or not the devices were actually beneficial to users, as opposed to other programs which largely rely on anecdotal evidence of improvement.

At the time of this publication, ARI is compiling the results of surveys presented to students when they were issued the devices and comparing them to surveys presented at the completion of the course.

Key Challenges and Lessons

Upon approval for the program, several key tasks and milestones were established, each meeting varied levels of challenge. Since the approval and purchase of the devices originated at Army CIO/G6 and the Army G8 level, it took less than 3 weeks to receive the 150 devices. At the time, three other areas still needed to be in place to bring the program up to the desired operation level, including the implementation of a commercial wireless network, the legal approval of an Apple Enterprise license for custom app distribution and the mobile device management solution.

Using on-hand wireless access points and connecting to an existing server stack used for code repository was easily accomplished with collaboration between the SIGCoE programmers and cadre at the Cyber Leader College in the 442nd Signal Battalion. The internal WiFi was not yet connected to a commercial network due to a local issue with the Internet Service Provider that connected the public Internet to Fort Gordon. In short, the company that provided those services had just been acquired by a different company and could not take on new clients until after the acquisition had been finalized. This left the SCPT in a time delay that lasted several months.

In the meantime, instead of leaving the tablets in wall lockers awaiting a public connection, we decided to issue the devices to the first class with the caveat that they would not be connected to the Internet during their class.

This allowed the SCPT to gather some control group statistics to answer the question, "Will the tablets, without connectivity, provide positive outcomes in the classroom?" As predicted, the students embraced the idea of having tablets as part of their course equipment, but without a connection found them to be extremely limited. Some used them to take notes and read PDFs that they could download from other Internet connections (home, hotel, coffee shop, etc), but found that the lack of connectivity in their classrooms did not encourage them to use the devices to the extent of their potential.

By the end of the first class, we had solved our ISP issues and deployed the local WiFi that allowed students to connect to the Internet. We still awaited approval of an Enterprise license to distribute custom apps experiencing three separate challenges. The first challenge was to get the Fort Gordon legal counsel to review the Enterprise developer agreement and determine who at the Signal Center could be authorized to bind the Center to the agreement. In this matter, we had considerable assistance from Apple's federal accounts managers for clarification on the terms and conditions, ultimately determining that a contractor officer Representative appointed by the contracting officer could sign the agreement. The second issue was that Apple requires a Data Universal Numbering System Number, which was something we didn't have specifically assigned to our unit. After some research, we were able to find a DUNS that we could put that would satisfy Apple's requirements. The final issue was simply paying the $299 for the fee. As a startup organization, we have

found that working through the processes to spend money is a very time consuming task for both small and large purchases.

Another challenge was adoption and acceptance within the schoolhouse. Although the SCCC leadership was enthusiastic and supportive of the SCPT, we were overly cautious about forcing the instructors, students and small group leaders into inserting too many components of the program into their classes and administrative features.

The result was that some areas that we thought should have been tested were not incorporated into the class. As an example, each student was given a wireless keyboard to assist with typing using the touch screen. One question we thought would be interesting to ask in a pretest was to determine students' thoughts about typing a 1000 word written assignment while using a tablet, then to ask them the same question at the end of the course. The hypothesis was that once a student used a wireless keyboard, trepidation about typing on the mobile device form factor would diminish. We suggested that the SCCC faculty require their students turn in one of their written assignments after writing the paper on the tablet. When we retrieved the first group of iPads, we were disappointed to find that many of the keyboards remained unopened and unused.

Despite this, the reaction to the inclusion of mobile tablets into the classroom was generally well received. In post class discussions, many of the students could clearly see the potential for mobile computing in a training environment and were eager to offer ideas of how the devices could be used in further classes. They were very interested in the ability to use tools that can assist them during their practical exercises, with access to the desktop and server applications at the top of their request list.

As the pilot is nearing its conclusion, we eagerly wait for the results from ARI to find the areas that were most positive in order to make a proposal for future efforts. While more work is required from security and policy perspectives, tt is clear from our observations that the inclusion of personal mobile computing in the military is in the future.

LTC Gregory Motes ***was the chief of the U.S. Army's Mobile Applications Branch at Fort Gordon, Ga, creating the concept for the SCPT program. LTC Motes spoke about mobile apps at several conferences or forums in the past 18 months and is one of the most influential people in Army mobility.***

CPT Chris Braunstein ***previously served as the lead engineer and automation management officer for the U.S. Army's Mobile Applications Branch at Fort Gordon. CPT Braunstein created a secure server infrastructure to allow connectivity between students and the Internet and has personally written 42 apps for iPhone or Android.***

Acronym QuickScan

AKO – Army Knowledge Online
AR – Army Regulation
ARI – Army Research Institute
AUP – Acceptable Use Policy
CAC – Common Access Card
CIO – Chief Information Officer
CPU – Central Processing Unit
DAR – Data at Rest
DECMAT – Decision Matrix
DUNS – Data Universal Numbering System
EAP-TLS – Extensible Authentication Protocol - Transport Layer Security
FOUO – For Official Use Only
iOS – iPhone Operating System
IP – Internet Protocol
ISM – Information Systems Management
ISP – Internet Service Provider
LAN – Local Area Network
Mbps – Mega Bits Per Second
MDM – Mobile Device Management
NIPRNET – Nonsecure Internet Protocol Router Network
OCSP – Online Certificate Status Protocol
OSI – Open Systems Interconnection
PII – Personally Identifiable Information
PKI – Public Key Infrastructure
PoE – Power over Ethernet
QR – Quick Response
RADIUS – Remote Authentication Dial In User Service
SCCC – Signal Captains Career Course
SCEP – Simple Certificate Enrollment Protocol
SCPT – SIGCoE Connected Personal Tablet
SIGCoE – Signal Center of Excellence
SNMP – Simple Network Management Protocol
SSID – Service Set Identifier
STIG – Security Technical Implementation Guide
USB – Universal Serial Bus
VLAN – Virtual Local Area Network
XML – Extensible Markup Language

Digital applications development training achieves big successes

By Donell Walker

One of the greatest successes from the Connecting Soldiers to Digital Applications initiative since 2010 has been the course designed to teach military members and government civilians how to write native applications for smartphones.

The program at the Signal Center of Excellence started with two assumptions. The first assumption was based the fact that Apple's App Store on iTunes had been active for just over one year and there were over 100,000 iPhone apps. Additionally, the Android marketplace's first few months also saw the rapid development and deployment of 20,000 apps.

The staggering rise of these two distribution channels suggested that developing apps was not too difficult. The second assumption was that the military has members in its ranks that have the ability to develop apps. This assumption was tested and proven true during the Apps for the Army Challenge, in which 53 apps were developed over a 75-day period.

As it turns out, developing applications is not as easy as first presumed - or at least it was not a task that could be picked up by that vast majority of our workforce with the same ease as, say, HTML. The complexity of quality native applications comes with a cost, which varies greatly throughout the industry and could range anywhere from $5K - $250K depending on the content, graphics, and cost of maintenance. From that came the question of whether or not the Army could create in-house capabilities for mobile app development? It was asked if the Army has Soldiers and civilians within the workforce who, with some development training, could become capable of developing and deploying mobile apps within training or operational contexts? From this question, the SIGCoE was tasked with examining the possibilities for providing instruction for mobile apps.

(Photo by Bonnie Heater)

The AN/TSC-185 STT appears on a Signal Soldier's Motorola Zoom Android Tablet after the QR Code for the equipment was scanned. This gives the Soldier access to the equipment user guides, training modules, maintenance manual, how-to-videos, technical manuals anywhere he or she may be.

The first question was to determine the appropriate population for mobile app instruction. Many years ago, the Army had Soldiers who wrote applications, but that task faded during the past 30 years. Within the professional military education system employed at the SIGCoE, the only course that engaged in any sort of programming was the Information Systems Manager's class that served as the functional area 53 qualification course.

At the time, the course had a five day section on programming in ASP.NET that was designed to satisfied the Critical Task and Site Selection Board task # 113-493-4000 to "Develop an Application". For that that task, the condition was: Given an operational requirement that cannot be met with a currently available COTS/GOTS solution, programming software, network, unit SOP, AR 25-1, AR 25-2, AR 380-5, AR 700-138, DA PAM 25-1-1, FM 3-0, and FM 5-0. The standard was: Create an application that satisfies the operational requirement IAW applicable regulations, policies, and procedures.

Furthermore, the following

subtasks were identified: 1. Develop the requirements for the application; 2. Select appropriate application tool(s) to develop the application; 3. Create application; 4. Conduct security and acceptance testing; 5. Deploy the application; 6. Document application; and 7. Maintain the Application.

When this task was approved by the CTSSB, it was obviously not specific to mobile applications, but the subtasks are clearly all components required in teaching mobile application development. Therefore, for the purposes of a pilot, it was determined that ISM students were the most likely student group to benefit from mobile application development.

LTC Gregory Motes was the chief of the Information Dissemination Management Division in the School of Information Technology and was asked to examine the difficulty of mobile app development and to formulate curriculum for a 5 day class.

After some initial examination into the skills required to write mobile apps, LTC Motes enlisted the assistance of CPT Chris Braunstein and CPT Stacey Osborn, who were "Snowbirds" (a colloquial term for students between courses) and had backgrounds in computer science.

The result was the development of curriculum for a five day courses for Android and iPhone that were presented to separate ISM courses in December 2010 and January 2011. Prior to these pilot courses, it was speculated that students attending the course would not represent a homogeneous population and would have a mix of students qualified to attend the class with those who did not have a background suitable for object oriented application programming. In fact, of the 23 students that took the initial iOS class, five students adequately absorbed the instruction and were able to grasp the difficult concepts at the end of the week. Another seven students could follow the instruction and were able to complete the exercises without too much difficulty. For the remaining students, the pace of instruction was extremely overwhelming. The Android class that followed had similar ratios among the 18 students.

The issue centered on the programming course's prerequisites. The civilian courses that the ISM training was modeled on usually required programming experience in an object oriented programming language such as Java (Android) and Objective-C (iPhone/iPad). Even the "iPhone for Dummies" book series required the reader to have a background in C or Objective C - which is hardly a "Dummy". As CSDA began to mature, organizations from inside and outside of TRADOC struggled to master mobile application development and numerous requests were made to the Mobile Apps Branch to hold a course. Civilian equivalent classes costs around $2,500 for 5 days of instruction (and more with travel and per diem), which was a cost barrier for a number of organizations.

This led the SIGCoE to create a ten day course that included one week in object oriented programming fundamentals, with a focus on Java for the Android courses and Objective C for the iOS courses, followed by a second week that we designed to teach specific programming tasks for the designated operating system. After sending out an email to the CSDA working group and other organizations that had been encountered during the first year of the CSDA program, 38 students were enrolled for the initial Android class. As a point of reference, a similar 10 day class in the civilian sector would have cost over $5,000 per student, for a total cost of $190,000.

The School of Information Technology was well equipped with computers and a student training network, allowing the students to each have access to the Integrated Development Environments and Software Development Kits used to program Android phones. Additionally, using a combination of VMware Lab Manager and virtual Windows 7 operating systems, students were able to access and store their work on a storage area network.

One principal change from this class and the ISM classes was that students were required to submit a short bio outlining any programming education or training that they may have had, which allowed the class administrators to determine the probability of each students success in the class. Students were also told that the course would be very challenging and requested only serious inquiries. Subsequently, several students who did not have a background commensurate with the requirements were not allowed enrollment.

At the completion of the first open class, three students actually published apps to the Android market, which demonstrated an immediate value to the course. This also led to an interesting talking point position where, on one hand, we were saying that writing apps is difficult and requires advanced training, but on the other hand we could point to the Army Values iPad app that took CPT Braunstein only four days to complete from inception to submission to the app store. It really validated the point that app development was not difficult for developers who had proper training. In CPT Braunstein's case, it was a computer science degree from the prestigious Rochester Institute of Technology.

On the other end of the spectrum was a handful of training developers and instructors who each presented information suggesting they had a background in programming. Their attendance at

(Continued on page 26)

(Continued from page 25)

an iPhone programming class left them realizing that previous experience in scripting, modular, functional and procedural programming languages was inadequate to quickly grasp object oriented programming.

Further refinement of curriculum and instruction were contracted through Technology Center Incorporation in Norcross, Georgia, which provided appropriate training materials for 10 day classes for iPhone and Android. Ultimately, the classes were set to consist of the following topics: Introduction to Programming using Java or Objective C, Getting Started with Android or iOS Programming, Displaying Maps, Activities and Intents for Android, Table Views, Application Storages, Animation and Video Playback, Network Access and a final project.

Over the course of the program, the SIGCoE held 8 courses, with an average of 25 students per class - essentially providing the equivalent of over $1,000,000 in training for a fraction of the cost. The last classes taught in June 2012 filled up 10 weeks prior to the start date and had a waiting list of students who were not allowed to attend due to the classes being fully booked. Students have attended from every corner of TRADOC, including active duty noncommissioned officers, warrant officers and officers, reservists, and DA civilians from each branch of the service. Furthermore, attendees have come from the White House Communications Agency, the Defense Information System Agency, and the Federal Bureau of Investigation. The vast majority of the students have been training developers who will take their training back to their organizations have begun to integrate mobile apps into their work where applicable.

As a side note, training was not limited to on site instruction, group instruction, or even native application development instruction. At various times, members from the SIGCoE traveled to an off-site location to conduct training, notably train-

(U.S. Army photo by SGT Michael J. MacLeod)

A paratrooper with the 82nd Airborne Division's 1st Brigade Combat Team uses a Handheld Interagency Identity Detection Equipment, or HIIDE, system to verify the identify of the Taliban leader they captured 26 Jan 2012, on the simulated battlefield of the Joint Readiness Training Center, Fort Polk, La. The system identifies people in a database that catalogs iris and fingerprint data.

ing 35 people at separate sessions during the 10th Annual Army distributed Learning Conference in 2011 where LTC Motes, CPT Braunstein and Donell Walker received the dL Maverick Award as "Out-of-the-box" thinkers. Additionally, training was conducted for 10 people in 2012 to achieved certification as Appcelerator Titanium developers, and additional training was gained in Blackberry OS, JQuery and PhoneGap to further round out the profile of technologies used for mobile apps. On other occasions, the SIGCoE mentored student projects at Augusta State University and the Army's Telecommunications Systems Engineering course, and even presented a lecture for students at Syracuse University's iSchool. The culture of learning and teaching has been a grand part of the success of the CSDA program.

One other topic that has garnered the attention of the SIGCoE was the release of iBooks Author software to develop eTextbooks for the iPad. Within days of the release of the free software, the SIGCoE had written a book to be used for demonstration at a CSDA working group and for publication onto Apple's iBooks. In April 2012, the SIGCoE hosted a workshop to teach training developers how to easily put content from their classes into an iBook, including text, pictures, image galleries, videos, audio, interactive images and additional widgets. Two very promising implementations are the inclusion of review questions that can be integrated within a books chapter and the ease at which instruction developers can incorporate a robust glossary for their students. Although the software is specific for iPads, there is an expectation that ePub formats for other mobile devices will catch up to allow other devices to display similar information.

Looking down the road toward adoption, acceptance and compliance of the Army's Learning Model 2015 and Army Training Model in TRADOC Pams 525-8-2 and 525-8-3, "requires a major change in the way the Army's trainers and training developers think about enabling training," specifying that the Army needs "tools that are low overhead, are mobile and capable of being interoperable and integrated, are reconfigurable, and which can be networked together quickly and seamlessly with joint and Army MCS." Current models for developing Interactive Multimedia Instruction and delivering content to personally owned electronic devices require deliberate consideration in a new era of fiscal challenges.

While there will be many occasions for organizations to write contracts to have mobile applications developed, there ought to continue to be a means to teach training developers and instructors how to create their own applications within the security and information constraints of the Army.

Donell Walker ***retired from active military service in 2004 after 21 years of service; 18 in the Information Technology field. During his military and civilian career, he has served in a myriad of technical positions to include computer operations, networking, information dissemination, training, and mobile applications development. He previously served as the Deputy and Operations Chief for the U.S. Army Mobile Applications Branch at Fort Gordon, Ga, playing a vital role in the team's development of approximately 100 applications with over 1.5 million downloads from the Apple App Store and the Google Play. Currently serves as the Battle Lab Collaborative and Simulation Environment Branch technical manager.***

Acronym QuickScan

AR – Army Regulation
ASP.NET – Active Server Pages (using .NET framework)
COTS – Commercial Off The Shelf
CSDA – Connecting Soldiers to Digital Applications
CTSSB – Critical Task Site Selection Board
DA – Department of the Army
FM – Field Manual
GOTS – Government Off The Shelf
IDE – Integrated Development Environment
IDMD – Information Dissemination Management Division
IMI – Interactive Multimedia Instruction
ISM – Information Systems Management
MCS – Maneuver Control System
OS – Operating System
PAM – Pamphlet
SDK – Software Development Kit
SIGCoE – Signal Center of Excellence
SIT – School of Information Technology
TRADOC – U.S. Training and Doctrine Command

Mobile device management

By CPT Christopher J. Braunstein

The modern era of computing has been shaped by the mobility revolution.

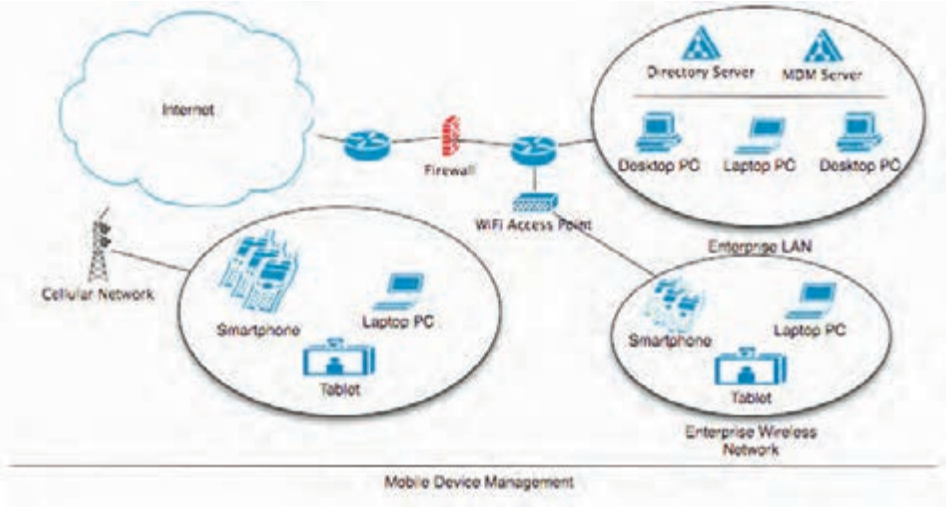
Desktops are beginning to fade in prominence as laptops, netbooks, ultrabooks, and other portable computers take over.

The pursuit of Moore's Law indicates that in the history of computing, the number of transistors that can be placed inexpensively on an integrated circuit doubles approximately every two years. This fact has resulted in an explosion of a new class of portable computers like Smartphones and tablets that are beginning to take hold in the enterprise.

Information technology departments have been flooded with radical new management ideas such as "Bring Your Own Device." Information assurance and computer security have become central concerns in every organization.

The challenges of managing a multitude of computing devices and maintaining the balance between security and usability become more complex every day.

Systems management has long been the cornerstone of enterprise-wide administration. A large organization like the Army has a clear requirement to create automated centralized processes to save time and money, increase productivity and application access, and provide a secure computing environment that minimizes risk. Management tools and processes have evolved from rudimentary programs such as shell scripts created by administrators into complex platforms and product lines. Solutions from multiple companies allow for security management, server availability monitoring, software inventory and installation, anti-virus and anti-malware management, network capacity and utilization monitoring, and user activity monitoring. Using a combination of these tools, an organization's managers can enact and enforce enterprise information technology policies and procedures.



Traditional desktop management evolved out of network management initiatives. Client desktops connected to local area networks that provided services required by users. These were often simple services like a corporate portal or file sharing. As software and operating systems evolved, the concept of a "managed desktop" became popular. Using Microsoft's Active Directory (or other open source tools such as Open Directory for Linux/Unix based computers) system administrators could apply policies to desktops. These policies could be linked to a user or to a particular policy. A managed desktop system could also provide authentication and authorization to all services included in a network.

Policies evolved over time allowing for fine-grained control over every aspect of the user's experience. Administrators could ensure a computer's software was up-to-date on patches and anti-virus definitions. They could remotely install new software on a group of desktops. Security could be enhanced by mandating password policies (or smart card authentication), disabling components of the operating system that were deemed unsafe, allowing users to only install and run approved applications, and actively monitoring the desktop's state. The policies could be applied to computer systems or to users and groups of users allowing great flexibility in the implementation of a desktop management corporate policy.

Over time, desktop computers faded and laptops became the hallmark of corporate use. Lightweight and portable laptops allowed traveling users to con-

tinue to get work done on the road. Administrators provided Virtual Private Network support to allow laptop users to connect to the corporate LAN and access services that were not publicly available on the internet. Desktop policy would be enforced and updated when the user connected their laptop to the VPN. Some risk was assumed as laptops were now able to be connected to external networks, losing the protection and monitoring ability of the corporate LAN when not connected to a VPN. System Administrators had to become more vigilant in enforcing IT policies and ensuring laptop computers were up to date.

Continuing along this theme, smartphones and tablets have arrived which bring ever smaller form factors that are highly portable to the fold. Cellular networks keep these devices attached to the internet continuously allowing for data consumption at any time, but also greatly expanding the risks of attack by malicious software and users. Mobile operating systems are often limited in their management capabilities (although this is improving quickly).

Traditional desktop management systems either do not support mobile devices or have a completely different way of management, as most mobile devices use operating systems that use different security models and systems than desktops. Mobile devices are difficult to track as they move on and off of a corporate LAN or change physical locations quickly. There are many different models, operating systems, and cellular network carriers adding to the complexity.

A new tool, Mobile Device Management, has evolved that can mitigate a lot of these risks. Mobile Device Management optimizes the functionality and security of a mobile device in relation to corporate policy; much like desktop management does in traditional IT settings. Typical MDM solutions include a server component that can send messages and commands to a mobile device, and a client component which runs on the handset or tablet and implements the commands. Newer solutions do not require a client component, as the client is embedded into the mobile operating system by the software or device manufacturer. The server solution can be hosted as a corporate service on existing infrastructure, or hosted through cloud services provided by the vendor.

In order to enable a device for management it must be provisioned. This process can vary from different vendor solutions, but it is commonly accomplished by visiting a web page or installing an application from a public market. Once this client application or configuration profile is installed the device is linked to the MDM console (which is often Web-based for ease of use). The MDM administrator can then push a profile to the device over the air that would alter the configuration of the device. The contents of the profile can include device settings, network and VPN configurations, account settings, security policies, password/passcode requirements, reporting requirements, and more. These profiles can also be sent to a group of devices or group of users, depending on what the administrator is trying to accomplish. MDM solutions often collect a lot of data from the mobile device.

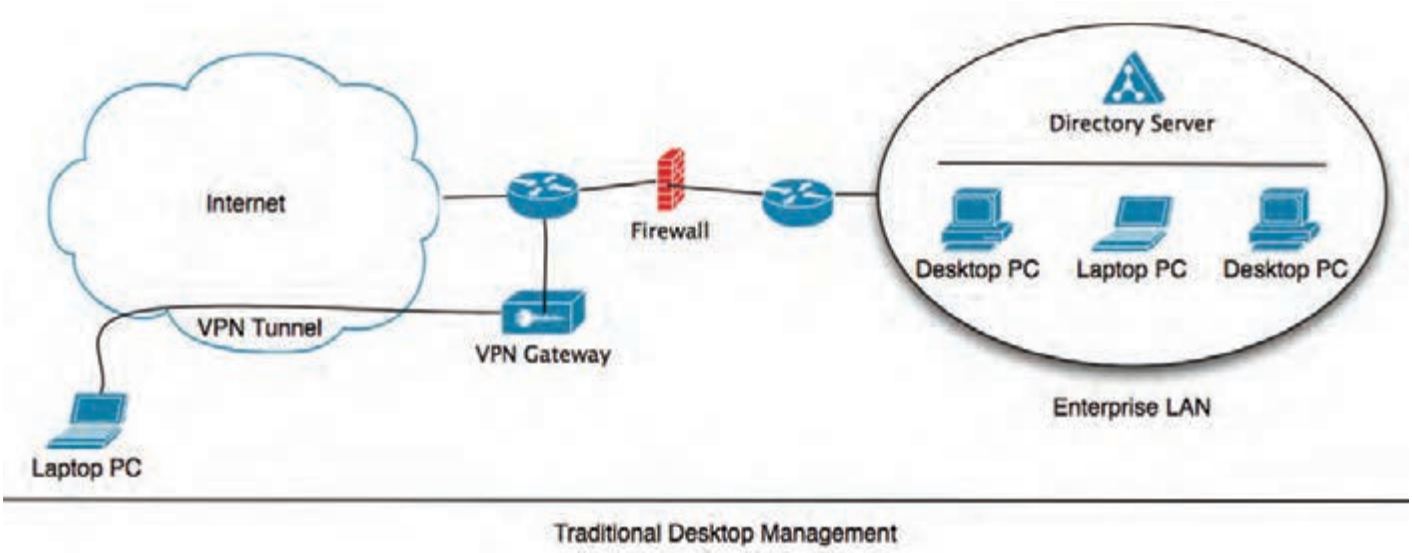
Global Positioning System embedded in the device is used for geo-location data. A summary of all settings and device conditions can be retrieved. A listing of messages/calls sent and received and their durations, software apps installed, and security state of the device can also be pushed to the MDM console. All of these things combined with the ability to control almost every aspect of the device's configuration leads to some interesting and novel thought about how to manage a network of computing devices.

An administrator can develop a system of profiles that increase or decrease permissions and security levels based not only on the user's authorization but also based on the state and location of the device or even the network to which it is connected. Tying these requirements to a digital certificate required for network or service access allows administrators to ensure users comply to a policy for a particular network or resource in order to connect.

For example, a user is issued a Smartphone, which is provisioned to use the MDM system. An initial profile is pushed to the user's device over the air (either an open corporate access point, or through the cellular network) that sets initial configuration settings and policies such as disabling the camera, creating a link to the corporate portal or app store, or adding email account or wireless network settings. The user is now able to connect the Smartphone to the corporate network and access services according to their authorization level. If the user requires access to a secure facility and corresponding network they could connect to the MDM system and request access. An automated or administrator controlled process could then push a new profile to the device with the new security settings (disabling wireless radios, GPS, app stores, etc.) that are required for that particular building or network. The user is then allowed to access those services as long as they are in compliance with that policy. The policy could also be set by location, i.e. a Sensitive Compartmented Information Facility would require a restricted profile that was automatically enabled and disabled upon entering and exiting by the system.

The addition of mobile devices to the Army Enterprise has often been impractical due to many factors

(Continued on page 30)



(Continued from page 29)

that MDM can solve. Using MDM in an enterprise solution such as the DISA DECC (much like Enterprise email) would centralize monitoring and security profile management. Access to administrative functions could be passed down to unit S6 sections, giving them powerful tools to rapidly provision, secure, track, and provide a true mobile data platform for our force. Inventory management could be simplified, as devices would be locatable through the MDM platform at all times. Lost or compromised devices could be remotely wiped by the MDM system, ensuring security of the networks and data that we use daily. As MDM continues to evolve it will most likely merge with and augment desktop management solutions, providing a holistic platform that administrators and commanders can use to ensure their network is providing necessary services in a secure and reliable manner.

CPT Christopher J. Braunstein *served as the lead software engineer for the Mobile Applications Branch, Accelerated Capabilities Division, Capability Development Integration Directorate, U.S. Army Signal Center of Excellence. CPT Braunstein led a team of programmers that have written nearly 100 applications for the iOS and Android platforms with over 1,500,000 downloads on iTunes and Google Play. CPT Braunstein is a graduate of the Rochester Institute of Technology with specializations in Computer Science and Information Technology. He worked for a Network-management focused consulting group as a software developer where he delivered solutions centered on the Simple Network Monitoring Protocol and network management automations. He was commissioned as an Armor officer in 2004 and served in various leadership positions to include forward support company commander, squadron adjutant, scout platoon leader, and assistant S3. CPT Braunstein deployed in support of Operation Iraqi Freedom 06-08. Upon redeployment he attended the Functional Area 53 (Information Systems Management) course, and the Signal Captains Career course.*

Join the Discussion
https://signallink.army.mil

Acronym QuickScan

DECC – Defense Enterprise Computing Center
DISA – Defense Information Systems Agency
GPS – Global Positioning System
IT – Information Technology
LAN – Local Area Network
MDM – Mobile Device Management
VPN – Virtual Private Network

HTML5 may provide vital link for friendly future mobile applications

By LTC Gregory Motes

An important thread that has existed in the background of the U.S. Army Training and Doctrine Command's Connecting Soldiers to Digital Applications program has been the desire to create applications that fell into the so-called "device agnostic" category.

As TRADOC leaders continue evaluating the role and viability of mobile devices in learning, training, and operational environments, a few goals have emerged. For example, we want to foster an atmosphere that sets priorities that limit duplication when creating applications that have financial and practical implications. Simply put, the best scenario is to be able to build training content once and to have it work across a maximum number of devices in both on-line and off-line states. To many, this would be accomplished with the maturation of HTML5.

The best scenario is to be able to build training content once and to have it work across a maximum number of devices in both on-line and off-line states. To many, this would be accomplished with the maturation of HTML5.

To fully grasp the opportunity, one needs to be aware of the history of HyperText Markup Language. In the early 1990s, Tim Berners-Lee created a new protocol called HyperText Transfer Protocol and a new text format markup language based on the Standard Generalized Mark-up Language. HTML notably added hyperlinks with an anchor element that carried an HREF attribute.

Over the next decade, HTML standardization, open standards and adoption engendered the modern Web site. Subsequent scripting languages, such as JavaScript, created a powerful tool for Web developers to create robust information and interactive Web sites. The power of HTML was its ability to interoperate on multiple browsers and platforms, providing users a similar experience without regard to their environment.

Yet, even this was not agnostic, as can be attested by people who chose to adopt new browsers and versions. Backward and forward compatibility created difficult challenges for developers - often exasperated in the Enterprise setting where adoption of new technologies had to undergo interoperability and security testing. The practical result within the military has been that systems and applications are often at least one version behind the current consumer offerings.

The crescendo of change that arguably started in 2007 when Apple announced the first generation iPhone has been growing louder as leaders and Soldiers have experienced the power of Smartphone's in their personal lives. The gap between potential capabilities offered by Android and iPhone/iPad and the technology presented in Army classrooms continues to increase as TRADOC examines fiscally sound ways to use the new medium. This has put training developers into a familiar "chicken versus egg" contest that seems to accompany many advances in technology. The question is raised about how to get funding for technologies that haven't previously been funded and how much time and existing resources should be used for pilot programs.

This evolution of technology has been particularly tricky due to the programming barriers that exist with creating native applications in iOS and Android. During the early stages of the CSDA program, a perception existed that developing Smartphone apps was not that difficult. This was likely based on the fact that there had been over 100,000 apps developed and published for the iTunes apps store after just one year. "How hard can it be?" Similarly, the new Android market (at the time) was also receiving a steady influx of apps. Still, the leap from programming in easier languages like HTML and Flash's ActionScript to object oriented languages like Objective C or Java was still a considerable one.

It should be noted that the rise of the native

(Continued on page 32)

(Continued from page 31)

app was unpredictable, even to Apple. Early documentation of the iPhone championed the rise of the web app and in fact did not have a substantial plan for native app development through a software development kit. The Internet still teems with web sites that gush about the potential for web apps using the new (2007) iPhone. Many of those sites, interestingly enough, return page not found results because, as it turns out, the web app was not the dawn of a new future for means to connect users to information and tools. Instead, in the shadows rose a community of hackers who began to reverse engineer certain parts of the iPhone operating system application programming instructions and created an underground market to distribute apps that perform functions not provided by the iPhone. In fact, Apple did not even have an app store, until 1 year after the release of the first version of the iPhone, and still hyped web apps.

At some point, Apple realized that there was a market for third party apps on iPhone - which is really no different from their allowing a mechanism to put third party apps on Mac - and started to court a developer community that quickly blossomed. The result was that production of web apps stalled, giving way to native apps. Yet, even the success of the native app, coupled with success of native Android apps, there is still an underlying clamoring for a standard language that can be written once and deployed everywhere. Native app development can range from cheap to expensive and from agile to cumbersome. Since the military has yet to choose Android or iPhone as its sole target for all apps (and likely doesn't intend on choosing one or another as the only solution for all cases), organizations that are interested in pursuing content delivery through a Smartphone are stuck with either choosing or having to develop for multiple platforms.

TRADOC can envision many different use cases for applications. One is the student in the classroom, the other is the student in the field, another is a student who is preparing to come to a professional military education course, and another is a graduate of a course. In an operational sense, Soldiers could use Smartphones to access information in environments that range from the orderly room, to the motor pool, to the clinic, and then into the field, whether it is training or in a combat environment. This makes isolating the environment an important part of the narrative. So, for a moment, just consider the Soldier who is preparing to attend formal military instruction and is required to take some training prior to arrival. This Soldier/student likely has access to a PC, but could also have access to a Smartphone or a tablet.

Prior to discussions leading to the Army Learning Model 2015, TRADOC's training developers were likely targeting just the PC and trying to account for multiple browsers if they were interested in reaching more users -- though most likely just targeting Internet Explorer. Even with creating modules in Flash that target a specific version of IE, it is a problem. At press time, the author of this article is working on a government computer that has Internet Explorer version 7.0.6 and Adobe Flash Player 11.2.202.228 Users at home likely have Internet Explorer version 9 (or are using Chrome, Firefox or Safari) and Flash Player 11.2.202.233. These discrepancies can return unpredictable results, creating the potential for interoperability, yet in a risk averse, low cost environment, these limitations are tolerated.

Modern Smartphone operating systems complicate matters even more. The goal of Smartphone "agnostic" applications has been an illusion, yet is still an idealistic goal that holds interest in communities like TRADOC that are trying to write once, deploy everywhere. It is with that, where HTML5 holds the promise of deploying content that will work across a maximum number of devices with limited interoperability issues, and in many ways filling the role that Flash has played in the past in the browser. As Flash has fallen out of favor as the de facto standard for interactive content on mobile devices - due largely to stability and power issues - HTML5 was increasingly presented as the alternate.

Between 2004 and 2009 groups within the World Wide Web Consortium developed positions and requirements for future hypertext application technologies, ultimately leading to the progression of a standard for HTML5. Some of the key components included improved graphics support with canvas and scalable vector graphics, wider multimedia support without the use of plug-ins, geo-location support within a web applications, and an application cache that could provide offline storage for apps. As an example, prior to HTML5, users could not draw on the web without the use of tools like Flash and Silverlight, but the ability to embed SVG into the document object model increase the capabilities presented to users natively in their browsers. HTML5 also offers a number of new APIs that will extend features that had to previously be programmed in other languages, including drag and drop, flexible parsing, system and directory access, and more robust error handling.

Yet for all of the interest, developers and users will still have to wait until 2014 for the entire HTML5 specification to be declared. It can be argued that the deliberate pace of implementation is prudent to come up with a lan-

guage that may bear the standard for 15 to 20 years, as its predecessor will have done, but is a source of frustration for those that are looking at it to be a viable alternative to native application development. Some browsers and applications already recognize HTML5 components. Notably, YouTube has a HTML5 implementation of its video player that tests fairly well despite certain restrictions. It is expected that browsers will gently include many of the HTML5 standards prior to the full specification, as is already available in the Webkit browsers that support certain HTML5 media tags already.

This interstitial period between desired effects and full scale implementation will continue to be bolstered by native app development, with an expected steady increase in applications that rely on HTML5. For mobile applications, several programs and development environments have gained momentum in allowing developers the opportunity to code in one integrated development environment and then have separate code compiled for different mobile operating systems. Among these, PhoneGap and Titanium are two notable efforts that have attempted to infiltrate the niche of developers that are trying to decrease the amount of work it takes to get an application onto multiple platforms. While both of these have certain strengths, the developer essentially has to learn another programming language (the appropriate API) and will likely experience a letdown trying to get the native look and feel they desire.

In the meantime, we have suggested that device "agnostic" apps are unlikely to appeal to the users who are infatuated with the user interface elements of their devices. Users on a PC will expect to have access to certain features by using the mouse right click or hovering over UI elements. Even though there have been some attempts at using a "long press" or a "two finger press" to bring up comparable menu options, the concept of hovering does not translate to touch screens. Furthermore, Android users have different expectations and anticipations than iPhone users. The most notable has been with the hardware menu button, where Android users will expect to be able to press that button during the operation of an app and be presented with additional menu options. This button does not exist on an iPhone, instead it is replaced by software buttons and tab-based navigation that is instantly familiar to its users. Blackberry's Playbook encourages developers to use gestures generated from the bezel to access additional information, which is again a concept that is unavailable for other devices. So, as developers are working toward creating an application that will work on a desktop pc, Android Smartphone, iPhone, Android tablet, iPad, or devices such as the Playbook, different user interfaces and programming logic will still exists.

HTML5 may eventually allow for an effective solution for developers to reach common denominators on devices and even account for different hardware capabilities using JQuery and CSS. Still, this promise is not going to eliminate the work of presenting standardized content on fragmented hardware while maximizing the potential of the leading tiers of consumer devices.

LTC Gregory Motes ***is an Armor Officer in Functional Area 53 Information Systems Management and is a doctoral candidate in Instructional Technology, examining situation awareness through a combat alert notification system. Over his career he has held a variety of leadership and staff assignments including tank company commander, MNF-I theater information assurance policy officer, division automation management officer and division chief at the School of Information Technology. He deployed his tank company to KFOR 2B, served in CFLCC and MNF-I for 16 months, and has 3 overseas assignments. He recently led the U.S. Army Mobile Applications Branch at Fort Gordon, Ga., which had a team of officers and contractors develop nearly 100 applications that received numerous awards and over 1,500,000 downloads on iTunes and Google Play.***

ACRONYM QuickScan

API – Application Programming Interface
CSDA – Connecting Soldiers to Digital Applications
DOM – Document Object Model
HREF – HyperText Reference
HTML – HyperText Markup Language
HTTP – HyperText Transfer Protocol
IDE – Integrated Development Environment
IE – Internet Explorer
iOS – iPhone Operating System
PC – Personal Computer
SGML – Standard Generalized Markup Language
SVG – Scalable Vector Graphics
TRADOC – U.S. Army Training and Doctrine Command
UI – User Interface
W3C – World Wide Web Consortium

NIE Network Integration Evaluation 12.2

(U.S. Army photo by Claire Heininger Schwerin)

(Above) **A Soldier from 2nd Brigade, 1st Armored Division demonstrates a Nett Warrior device during NIE 12.2. As part of Capability Set 13, Nett Warrior is a Soldier-worn, Smartphone-like mission command system that connects with the JTRS Rifleman Radio to provide dismounted leaders with increased situational awareness and mission-related "apps."** *(Right)* **A 2/1 AD Soldier stands before a Warfighter Information Network-Tactical Increment 2 Point of Presence on May 17, 2012 during the WIN-T Increment 2 Initial Operational Test and Evaluation at White Sands Missile Range, N.M. Held in conjunction with the Army's Network Integration Evaluation 12.2, the three-week WIN-T Increment 2 IOT&E was conducted in May in real-world operational environments, including WSMR's deserts, mountains, and a simulated urban village as shown here.**

(U.S. Army photo by Amy Walker)

(Above) **The brigade Tactical Operations Center was the operations hub during the Network Integration Evaluation 12.2, which was held in conjunction with the Warfighter Information Network-Tactical Increment 2 Initial Operational Test and Evaluation. The structure of the brigade TOC consisted of the Standardized Integrated Command Post System Trailer Mounted Support System - Large. The TMSS-L combines shelter, utilities, power, environmental control and tactical mobility to form a complete command operation center. During the event the brigade TOC, which contains dozens of network systems, "jumped" or moved three times, tested mission command on-the-move capabilities, and then reestablished connectivity to full operational capability.**

(U.S. Army photo by Amy Walker)

(U.S. Army photo by Claire Heininger Schwerin)

(Above) **A Soldier from 2nd Brigade, 1st Armored Division moves into position in front of vehicles equipped with Warfighter Information Network-Tactical Increment 2 during the Network Integration Evaluation 12.2 at White Sands Missile Range, N.M., in May. With the 3,800 Soldiers of 2/1 AD conducting a rigorous, intelligence-driven operational scenario against a battalion-sized opposing force, the Army's new tactical communications network allowed them to rapidly pass information across echelons -- from the brigade tactical operations center down to the individual Soldier. Facing a hybrid threat comprised of conventional forces, insurgents, criminals and electronic warfare, the brigade executed combined arms maneuver, counterinsurgency and stability operations.** *(Below right)* **A 2/1 AD Soldier uses the Joint Tactical Radio Systems Rifleman Radio to communicate during the NIE 12.2. The Rifleman Radio, a two-pound radio carried by the individual Soldier for voice communications and to transmit position locating information. Used by team leaders and above, the Rifleman Radio can also link with handheld devices to transmit text messages, GPS locations and other data.** *(Below)* **The NIE 12.2 was the third and largest such event the Army has held to date, requiring the 2nd Brigade, 1st Armored Division to assess the network's performance while stretched across vast distances and punishing terrain at White Sands Missile Range. Soldier feedback and test results from NIE 12.2 will validate and finalize Capability Set 13, the first integrated package of tactical communications gear that will be fielded to eight brigade combat teams starting in October 2012.**

(U.S. Army photo by Claire Heininger Schwerin)

(U.S. Army photo by Claire Heininger Schwerin)

509th Signal Battalion Launching Next Generation VoIP System

By Todd C. Hunt

In July of 2012 the 509th Signal Battalion will launch a next-generation Voice over Internet Protocol system designed to provide Defense Switched Network dial tone services at the new U.S. Army installation on Dal Molin.

The $2.8 million IP telephony project is part of an effort to stand up world-class voice and data services for Army Europe's largest military construction project currently underway in Vicenza, Italy.

Located on the Northwest side of the city of Vicenza, the Dal Molin campus falls within the greater Vicenza Military Community. The $430 million green-field installation will be home for elements of the 173rd Airborne Brigade Combat Team and Headquarters U.S. Army Africa. Consolidation of the Airborne Brigade on Dal Molin in the spring of 2013 is expected to add 2,300 Soldiers to the Vicenza population.

With the Cisco Unified Call Manager enclave programmed for activation this summer, the battalion intends to have future Dal Molin customers fall in on a well-established, fully-accredited VoIP network.

The 509th Signal Battalion presently provides DSN services to more than 5,000 customers across Northern Italy and the Balkans. Current DSN architecture in the region includes a mature network of class-5 TDM end offices consisting primarily of Siemens EWSD and HiPath systems.

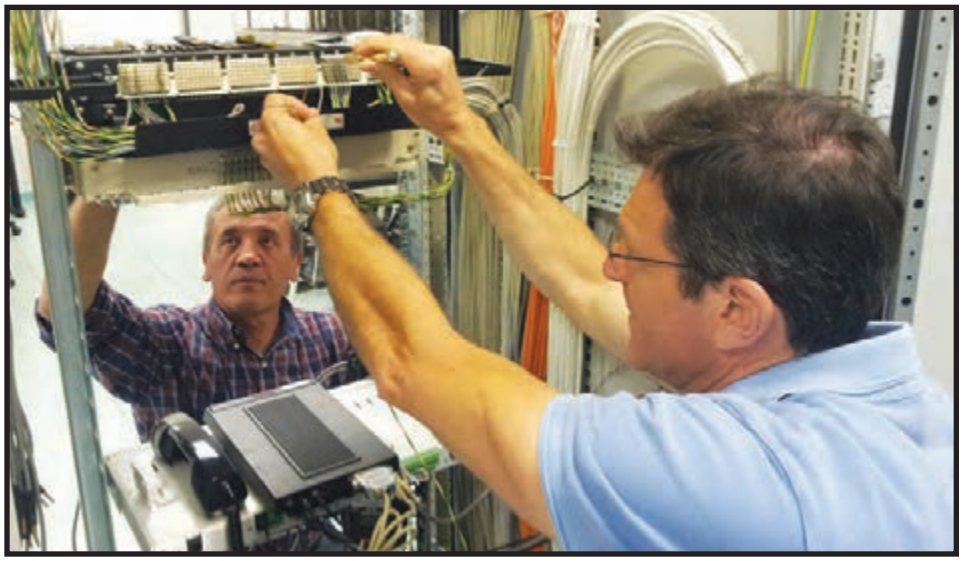
After nearly 10 years in operation, the highly-reliable Siemens systems have provided significant return on investment. Although similar TDM systems were initially considered for the Dal Molin campus, a business case to support further development of the legacy technology could not be established. Instead, designers opted to explore emergent IP-based solutions in an effort to reduce infrastructure cost and avail of an array of enhanced capabilities.

The decision to pursue a VoIP solution in Italy did not come without some controversy. With enterprise and theater Unified Communications initiatives in the initial planning stages and a HQDA CIO/G6 moratorium placed on standalone VoIP enclaves, the desire for IP telephony service on Dal Molin could not have come at a more inopportune time. Overarching UC programs did not sync with the Dal Molin implementation schedule and TDM-based systems were no longer available on the JITC approved products list. Unable to align end-state design criteria with the construction timeline, project managers were forced to consider interim solutions.

In November of 2009, provisional VoIP services were fielded for the construction offices on Dal Molin leveraging the Transportable Voice over Internet Protocol Switch, also known as TVIPS. In addition to its versatility the TVIPS had the advantage of a valid accreditation and fit the interim needs at Dal Molin without issue. This initial VoIP installment was sized to bridge the gap between the construction phase and the deployment of full-scale voice services.

Despite its limited capacity, TVIPS proved to be the right thing at the right time. In the two years following its activation services were extended beyond Dal Molin in support of contingency operations and to remote DSN users across the region.

With the provisional system firmly in place, the 5th Signal Command engineering staff was able to turn its attention to the planning of a permanent voice network solution for the new campus. Synchro-



Raffaele Fusco ***(left)*** **and Mirco Finco install T1 connections between the Electronic Worldwide Switch Digital switch and the Message Gateway Control Protocol routers.**

Luciano Poli adds Cisco IP phones to the Cisco Unified Communications Manager database in preparation for the TVIPS user migration.

nizing efforts with the servicing signal battalion, the command developed a follow-on VoIP strategy that would scale into future enterprise and theater architectures.

In July of 2011, engineers completed installation of a PBX-1 CUCM enclave designed to provide high-availability VoIP services on the Dal Molin campus. Planned with future expansion in mind, the system was built with sufficient capacity to support all users across the 509th Signal Battalion footprint.

The initial VoIP implementation will provide capabilities similar to existing TDM systems with a few highly-desired enhancements. Augmented by Cisco's Unity Connection package, the Dal Molin VoIP enclave will offer voicemail as a baseline DSN service for the first time in the region. Other features distinguishing the follow-on VoIP system from its TDM predecessor include Extension Mobility, a web-based user interface, as well as enhanced Ad-Hoc and Meet-Me conference bridging.

As Dal Molin is integrated in the developing enterprise UC design, the door will be opened to the full range of converged network capabilities. Functionality such as Active Directory Integration, Unified Messaging and Global Directory services will fundamentally transform the basic VoIP network as USAREUR's southern flank is progressively incorporated in theater, enterprise and global UC architectures.

Users will be migrated to the Cisco Unified Communications Manager in three distinct stages beginning with the phase out of the provisional TVIPS system. The initial stage will transition more than 150 customers, dispersed across Italy and the Balkans, to the Cisco VoIP enclave. Phase two will integrate PBX-1 CUCM services across the Dal Molin, Caserma Ederle and Livorno campus area networks. In the final stage, the stand-alone VoIP enclave will be merged with the theater UC network followed by the migration of inter-site call routing from legacy PCM trunks to the IP cloud. To achieve this, the PBX-1 installation will be reconfigured as a LSC and AS-SIP trunks will be provisioned to Multi Function Soft Switches in the Central and Southern European region. The final stage will also include advancements to security with the realization of SRTP between all participating VoIP endpoints.

Customer and service provider alike anxiously await the ribbon cutting ceremony this July that will launch Army Europe's largest all-VoIP campus. This momentous event marks a giant leap from basic dial tone services to a highly-versatile converged voice and data network architecture. The long road to VoIP has led to the design of a solid Unified Communications foundation and the development of an incremental plan for expansion of services as enterprise initiatives mature. The collaborative efforts of the 5th Signal Command and 509th Signal Battalion teams have once again delivered a world-class technology solution to our war fighters in the Southern European region.

Todd Hunt, ***a retired U.S. Air Force veteran, is a Department of the Army civilian serving as the chief of the 509th Signal Battalion's Network and Switch Division. He has over 28 years of experience in the communications and information technology arena with key assignments to NATO, Air Force Space Command and Headquarters 16th Air Force. His project portfolio includes contributions to the Defense Information System Network-Europe, Space Based Infrared System and U. S. Atomic Energy Detection System programs as well as an array of Global Information Grid test and evaluation initiatives.***

Acronym QuickScan

AS-SIP – Assured Services Session Initiation Protocol
CIO – Chief Information Officer
CUCM – Cisco Unified Communications Manager
DSN – Defense Switched Network
EWSD - Electronic Worldwide Switch Digital
HQDA – Headquarters Department of the Army
IP – Internet Protocol
JITC – Joint Interoperability Test Command
LSC – Local Session Controller
PBX-1 – Private Branch Exchange 1
PCM – Pulse Code Modulation
SRTP – Secure Real-time Transport Protocol
TDM – Time Division Multiplex
TVIPS – Transportable Voice over Internet Protocol Switch
UC – Unified Communications
UC – Unity Connection
USAREUR – United States Army Europe
VoIP – Voice over Internet Protocol

Virtualization beneficial as a platform

By Charles I. Calabrese

The technology of server infrastructure and the demand of information technology to support the warfighter have been growing at an astronomical rate. The need to provide systems and services for intelligence and mission command exists on the battlefield, and as well as posts, camps and stations.

In order to provide these services 5th Signal Command, with the direct support of the 509th Signal Battalion provides an Installation Processing Node – Italy which comprises of Army Non-secure Internet Protocol Routing Network and Secure Internet Protocol Routing Network services. Due to the increased demand of systems and services the IPN-I has had to re-engineer the way that services are provided to the customer.

Taking a first step into the technology of virtualization, the 509th Signal Battalion, Systems Support Branch has worked hand in hand with the Knowledge Management Office of U.S. Army Africa Command to provide a high availability with a data recovery site in order to support mission and automation needs. USARAF has become reliant on the use of Microsoft SharePoint Portal and the SSB took on the mission to design, test, implement, and maintain the services.

By designing the virtual infrastructure the SSB was able to consolidate physical servers; which not only reduced the footprint to the facility, but reduced the power and HVAC requirements needed to provide the systems to the community.

Finalizing the testing phase, the SSB has taken this to the next level with Caserma Del Din, formerly Dal Molin, coming on board FY13. Additionally the move of the IPN-I facility to Caserma Del Din, there were additional requirements that needed to be looked at to ensure that the transition to the new facility would not have an impact on the services being provided by the 509th Signal Battalion.

The SSB designed virtual clustered services for Structured Query Language, Dynamic Host Configuration Protocol, print services, and file services that will allow complete service failover to the Continuity of Operations Plan site during the transition. The services that cannot be clustered, like Microsoft SharePortal and web application servers will use live migration features built into Microsoft's Hyper-V server clustering technology. This allows services to be moved between clustered Hyper-V servers without an interruption of service to the customer. The design of the virtual infrastructure ensured that there was no single point of failure; this included working with the 509th Signal Battalion Network Services branch to assist in the design of the meshed networking architecture to support failover and redundant network paths.

Virtualization technology has also required the SSB to look at the way it backs up systems, with virtual servers, restoring operating systems takes minutes as opposed to hours. What this means is rapid recovery on services to the customer with the least amount of operational impact.

Converting services to the new virtualization infrastructure will allow the 509th Signal Battalion to provide an equivalent enterprise level of service to the customers within the Vicenza and Livorno Military Communities for mission funded services, along with other critical non-enterprise servers that are normally provided by the local signal battalion. Being able to provide this level of service was impossible before the advent of virtual technology and the hardware to support such a capability.

Virtualization as a platform is the future of providing services to the customer, with the processing power of today's servers, there is no reason not to implement the technology. The cost savings alone for power, HVAC, and facility space supports the reduction of government spending and sustainment requirements. The benefits of providing a faster recoverable and failover platform is being successfully used in the commercial market and the military has adapted the same processes as a way to provide the increasing service requirements without the additional cost to implement and sustain them.

By staying on the cutting edge of information technology, the 509th Signal Battalion has provided the command with more robust and responsive network services, while simultaneously conserving Army resources. This is a good news story for all.

Charles Calabrese ***retired from the U.S. Army Signal Corps as a senior noncommissioned officer. As a Department of the Army civilian, Mr. Calabrese deployed to Afghanistan in support of the Army's Southern European Task Force and Combined/Joint Task Force-76. He is currently the chief, Desktop & Systems Support Division for the 509th Signal Battalion headquartered at Caserma Ederle, Italy.***

Acronym QuickScan

FY - Fiscal Year
HVAC - Heating, Ventilation and Air Conditioning
IPN-I - Installation Processing Node-Italy
KMO - Knowledge Management Office
NIPR - Non-secure Internet Protocol Routing Network
SIPR - Secure Internet Protocol Routing Network
SSB - Systems Support Branch
USARAF - U.S. Army Africa

Female Signal Soldier sets historical mark at The Citadel

By Lt. Col Mark Rosenstein

SFC Kristen Nelson, a Signal Soldier recently made history by becoming the first Army female NCO to serve as permanent cadre at the Citadel in Charleston, S.C.

An official statement from the U.S. Army Human Resources Command, Signal Enlisted Branch offered congratulations to SFC Nelson a 25U Soldier. "Her selection exemplifies her outstanding performance and future potential to the Regiment and our Army."

SFC Nelson was born in Dudley, Mass where she attended Shepherd Hill regional high school. She entered active duty in 1996, attended basic training at Fort Jackson, S.C. and graduated Advanced Individual Training as a 25U, Signal Support System Specialist, from Fort Gordon, Ga. Her duties have taken her around the country and world. At Fort Drum, N.Y. she served as a retransmission team leader, Signal support systems team chief, battalion S-3 schools NCO, and an information systems operator-analyst. At Fort Gordon she served as an instructor/writer. At Fort Leonard Wood, Mo. she served as a senior drill sergeant and at Fort Stewart, Ga., she served as a communications chief. In 2009, she deployed to Iraq in support of Operation Iraqi Freedom and Operation New Dawn.

Her military education includes the Warrior Leadership Course, the Advanced Leaders Course, the Senior Leaders Course, the Drill Sergeant School, the Total Army Instructor Course, the Equal Opportunity Leaders Course, and the U.S. Air Force Airlift Planner Course. Her civilian education includes an Associate of Science degree in early childhood education.

Her service is recognized with the Bronze Star Medal, the Army Commendation Medal with two oak leaf clusters, the Army Achievement Medal with two oak leaf clusters, and the Army Good Conduct Medal among others.

SFC Class Kristen Nelson serving as the 26th Signal Brigade Support Battalion S-6 communications chief.

In her own words

"I initially joined the Army to further my educational goals, however, I now find that the Army provides me with a rewarding environment to learn, grow, and lead. My continued service in the military allows me to support my family while serving my country. I joined the Signal Corps because it afforded me the best opportunity to contribute to the mission. I felt that a job in communications would suit me best. Army communications was on the cutting edge of technology, was oriented towards the future, and was my number one choice for military service.

My most memorable experiences include being a drill sergeant where I had the privilege of training civilians and making them into Soldiers and deploying to Iraq where I had the honor of serving our country in combat and the responsibility of ensuring every member of my S-6 team returned safely. I look forward to continuing to grow as an NCO, serving as a first sergeant and becoming a command sergeant major. The Army has undoubtedly made me a better person and leader."

Join the Discussion
https://signallink.army.mil

City honors former Chief of Signal

(Photo illustration by Nick Spinelli)

By Nick Spinelli

Leaders and members of the Fort Gordon and Central Savannah River Area communities gathered on Walton Way in Downtown Augusta, Ga., June 5 for the dedication of a bridge named in honor of LTG Robert E. Gray, who was killed in a traffic accident in November 2011.

"It is only fitting that we honor him in this way," said Rev. Larry Fryer of Hudson Memorial Christian Methodist Episcopal Church, "since this man has been a bridge for so many in life."
Lt. Gen. Gray served as Fort Gordon's commanding general from 1991 to 1994, and eventually became an active member of the CSRA community after his retirement in 1997.

Dr. Lowell Greenbaum, a close friend of Gray's, said the general, "not only served his country but served as a beacon of humanity within the community."

Fort Gordon Garrison Commander COL Robert A. Barker addressed the impact Gray had on servicemembers and civilians alike during the ceremony.

"His ability to touch lives is an indicator of his great character," Barker said. "When we look at his life, we see a man who demonstrated that he wanted to make a difference. We acknowledge the significance of his life and magnitude of his accomplishments."
Augusta Mayor Deke Copenhaver also addressed the audience, echoing the significance of Gray's memorial being a bridge.

"Where others tried to put up walls, he built bridges and blazed trails," Copenhaver said.

When it was her turn to speak, Gray's wife, Annie – accompanied by her daughter Frances – thanked the community. She told the assembled audience how grateful she was for the honor being bestowed on her husband and how touched she felt to have so many people in attendance celebrating his memory.

"Thank you all so much," she said. "I know he would be proud of this."

Nick Spinelli ***is a writer/editor with the Fort Gordon Public Affairs Office at Fort Gordon, Ga.***

New Training Products and Equipment Information:

- PSC 5 Shadowfire Training Material and Software
- BFT Joint Capabilities Release Training Material
- KGV-72 Training Material
- 25P10 Microwave Systems Operator Interactive Multimedia Instruction (IMI)
- Phoenix AN/TSC-156 Delta Simulator
- TRC 170A (V3) Tropo Simulator
- WIN-T Increment 1 New Equipment Training (NET) Courseware
- Battle Command Common Services (BCCS) Interactive Multimedia Instruction (IMI)

Also:

- Tactical Radios (PRC/PSC/ARC/FBCB2/HCLOS...)
- JNN/WIN-T Training
- Mission Command (Battle Command) Systems

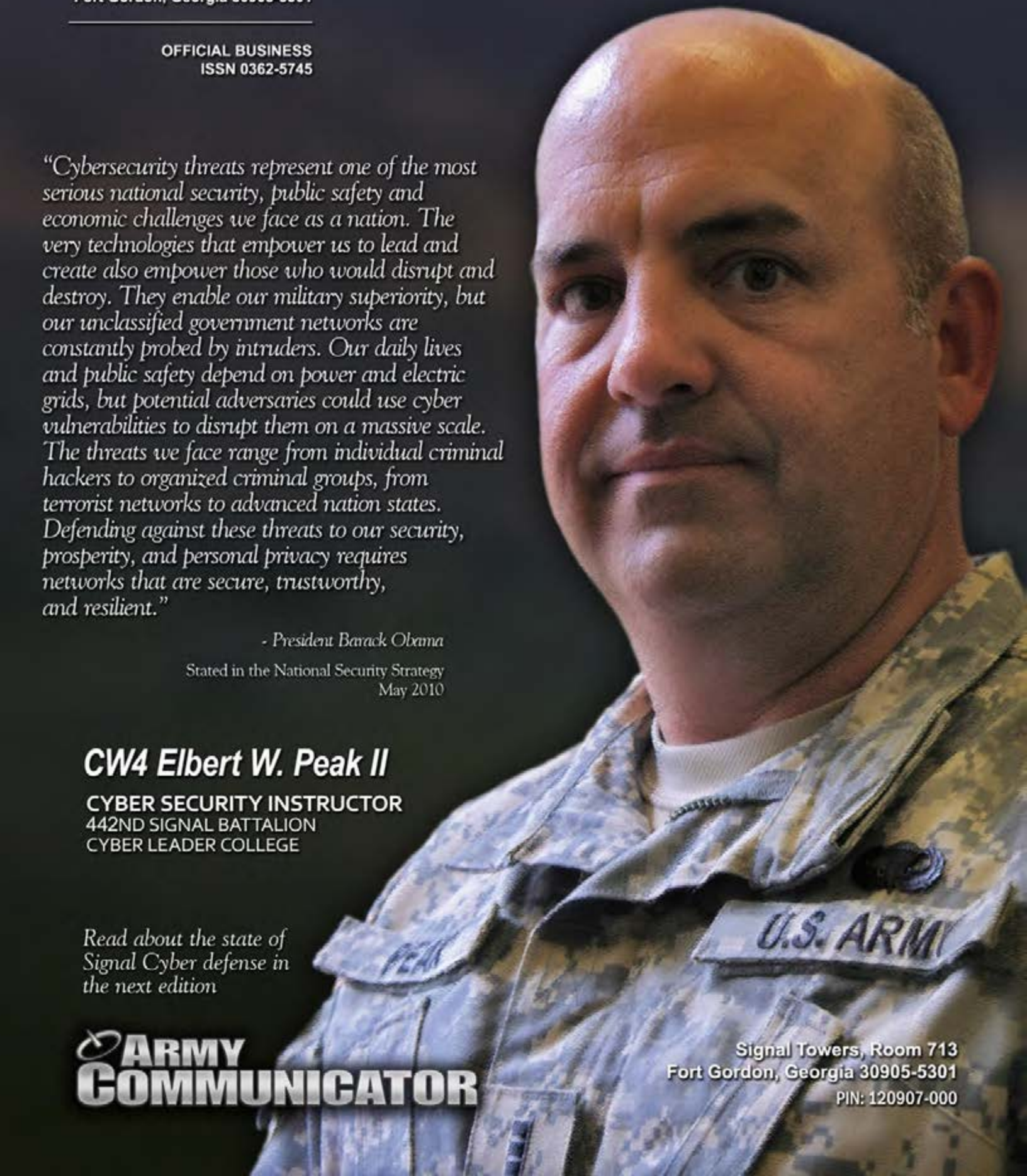
And much, much, more at **LandWarNet eUniversity**

LWN.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



"Cybersecurity threats represent one of the most serious national security, public safety and economic challenges we face as a nation. The very technologies that empower us to lead and create also empower those who would disrupt and destroy. They enable our military superiority, but our unclassified government networks are constantly probed by intruders. Our daily lives and public safety depend on power and electric grids, but potential adversaries could use cyber vulnerabilities to disrupt them on a massive scale. The threats we face range from individual criminal hackers to organized criminal groups, from terrorist networks to advanced nation states. Defending against these threats to our security, prosperity, and personal privacy requires networks that are secure, trustworthy, and resilient."

- President Barack Obama

Stated in the National Security Strategy
May 2010

CW4 Elbert W. Peak II

CYBER SECURITY INSTRUCTOR
442ND SIGNAL BATTALION
CYBER LEADER COLLEGE

Read about the state of Signal Cyber defense in the next edition

ARMY COMMUNICATOR

Signal Towers, Room 713
Fort Gordon, Georgia 30905-5301
PIN: 120907-000