

# ARMY COMMUNICATOR

Voice of the Signal Regiment

PB 11-15-1 2015 Vol. 40 No. 1

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



ENABLING SUCCESS FOR  
TODAY AND TOMORROW



# Chief of Signal Thomas A. Pugh

## Enabling Success for Today and Tomorrow

This edition of the *Army Communicator* highlights the global, enterprise and expeditionary nature of our operations while fully acknowledging our newly selected distinguished members of the Regiment and their massive contribution to our history. I invite you to read the article to familiarize yourself with our "Chief of Signal Awards Program" and use it to continue to recognize the superb individuals of our Signal Corps.

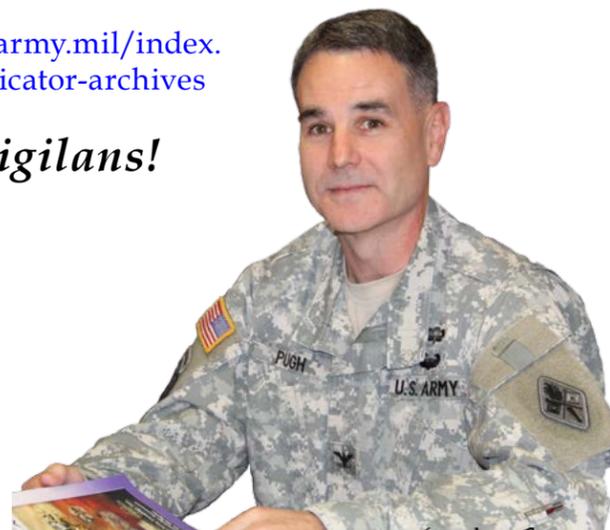
Throughout our history the strength of the Signal Corps has been the ability to innovate and adapt. Every day in the news you hear about the impact the Cyberspace operational environment is having on our military operations, our Nation and our world.

The Signal Corps is poised to be THE major contributor to the Cyberspace operational domain and will require us to be ever more adaptive and innovative in the future. We have a demanding future ahead of us and change must be a part of our culture.

The *Army Communicator* is your publication and I invite you to write articles and contribute to the dialog and pass it along to others for their professional development. Current and past issues are available online at:

<http://www.signal.army.mil/index.php/army-communicator-archives>

*Pro Patria Vigilans!*



*Thomas A. Pugh*

U.S. ARMY SIGNAL SCHOOL  
FORT GORDON

### COMMAND

Chief of Signal  
COL Thomas A. Pugh

Regimental Chief Warrant Officer  
CW5 Peter T. Winter

Regimental Command Sergeant Major  
SGM Aaron Prater

### EDITORIAL STAFF

Editor-in-Chief Larry Edmond  
Technical Editor CPT Damon N. Knauss

Art Director/Graphic Designer  
Billy Cheney

Photography  
Billy Cheney, J.D. Leipold, CPL Cansin P. Hardyegritag, CPL Sean Scarfus, SSG Kevin Iinuma, SSG Michael Folkert

By Order of the Secretary of the Army

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

Official:

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

Authorization 1516102

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

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

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

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

*Army Communicator* reserves the right to edit material.

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

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

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

# ARMY COMMUNICATOR

Worldwide web homepage address  
<http://www.signal.army.mil/ococ/AC/>  
E-mail: ACeditor@conus.Army.mil

PB 11-15-01  
Spring 2015  
Vol. 40 No. 1

## Voice of the Signal Regiment

### Features

- |  |   |
|--|---|
| <p>2 <b>The Army Network Enabling Success for Today and Tomorrow</b><br/>LTG Robert Ferrell<br/>COL Linda Jantzen</p> <p>7 <b>The Cloud-enabled Network</b><br/>COL John Rozsnyai</p> <p>12 <b>JBSA Massive Network No Longer a Dream in the Cloud</b><br/>Dennis Garrison</p> <p>13 <b>Command Post of the Future Evolves</b><br/>Kathryn Bailey</p> <p>14 <b>U. S. Central Command Managing Complex Challenges</b><br/>BG Peter A. Gallagher</p> <p>21 <b>African Command enabling diverse partners</b><br/>COL Patrick Dedham</p> <p>24 <b>AFRICOM provides Ebola Response Communications</b><br/>LTC Matthew J. Foulk<br/>MAJ Joseph L. Heyman<br/>CW2 Reba Wallner</p> <p>32 <b>From 'Mixed Signals' European Command brings together Allies</b><br/>MAJ Natalie Vanatta<br/>CPT Robert Singley and<br/>CPT James Torrence</p> <p>38 <b>2015 Regimental Signal Corps Ball</b></p> | <p>40 <b>All you need to know About the Chief of Signal Awards Program</b></p> <p>42 <b>New Distinguished Members of the Regiment</b></p> <p>52 <b>Signal History Moment Amazing Grace</b><br/>Steven J. Rauch</p> <p>55 <b>Wig-Wag or Semaphore</b><br/>Daniel A Brown<br/>Steven J. Rauch</p> <p>59 <b>DISA Shaping the Joint Information Environment</b><br/>Kitsy Young</p> <p>61 <b>DISA supports Unified Capabilities Implementation</b><br/>Andy Bryczek</p> <p>63 <b>Next Generation IT Procurement</b><br/>MAJ Alexander Vukcevic<br/>Michael R. Grimaila</p> <p>73 <b>7th Signal Command (T) Fielding Signal/Cyber Teams</b><br/>MG John W. Baker</p> |
|--|---|

### Join the Discussion

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

~On the Cover~

**Networks to the Edge**  
Soldiers in the Signal Corps are on the ground, advancing a vastly distributed mission command system as the Army continues making communications more reliable, mobile and agile thanks to smaller, lighter network components with lower power and cooling requirements, coupled with a robust network infrastructure that has greater capacity and flexibility.



Cover design by Billy Cheney

~Status Reports~  
In this issue read updates from Signal units that are working around the globe to establish, maintain and secure the networks essential to global operations.



CIO/G6  
Page 2



USCENTCOM  
Page 14



AFRICOM  
Page 21



USAREUR  
Page 32  
and more...

Enabling Success for Today and Tomorrow

# The Army Network

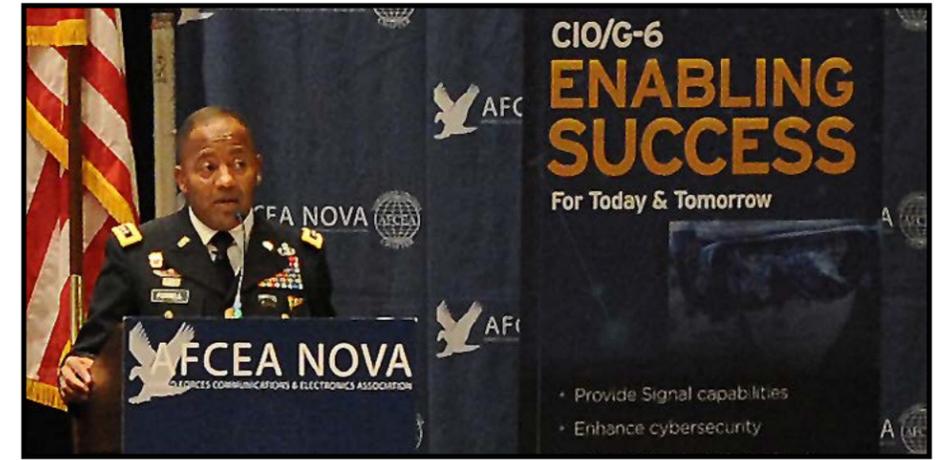
By LTG Robert S. Ferrell  
and  
COL Linda Jantzen



is many things to many people, depending on how, when and for what purpose it is used. It is at once a business and collaboration tool, a training enabler and a warfighting platform. The network is the entry point to the cyberspace domain and simultaneously enables maneuver across all other domains. Whether you are working in a headquarters at home station, training with your unit in the field or deployed to a combat zone, a secure, flexible and resilient network that provides access to the information you need is a critical enabler for success *in every mission in any environment.*

LTG Robert S. Ferrell, Army Chief Information Officer/G-6, announces the implementation of the Army's Network Campaign Plan during the 14th Annual Armed Forces Communications and Electronics Association's Northern Virginia Army IT Day, 4 Feb. 2015.

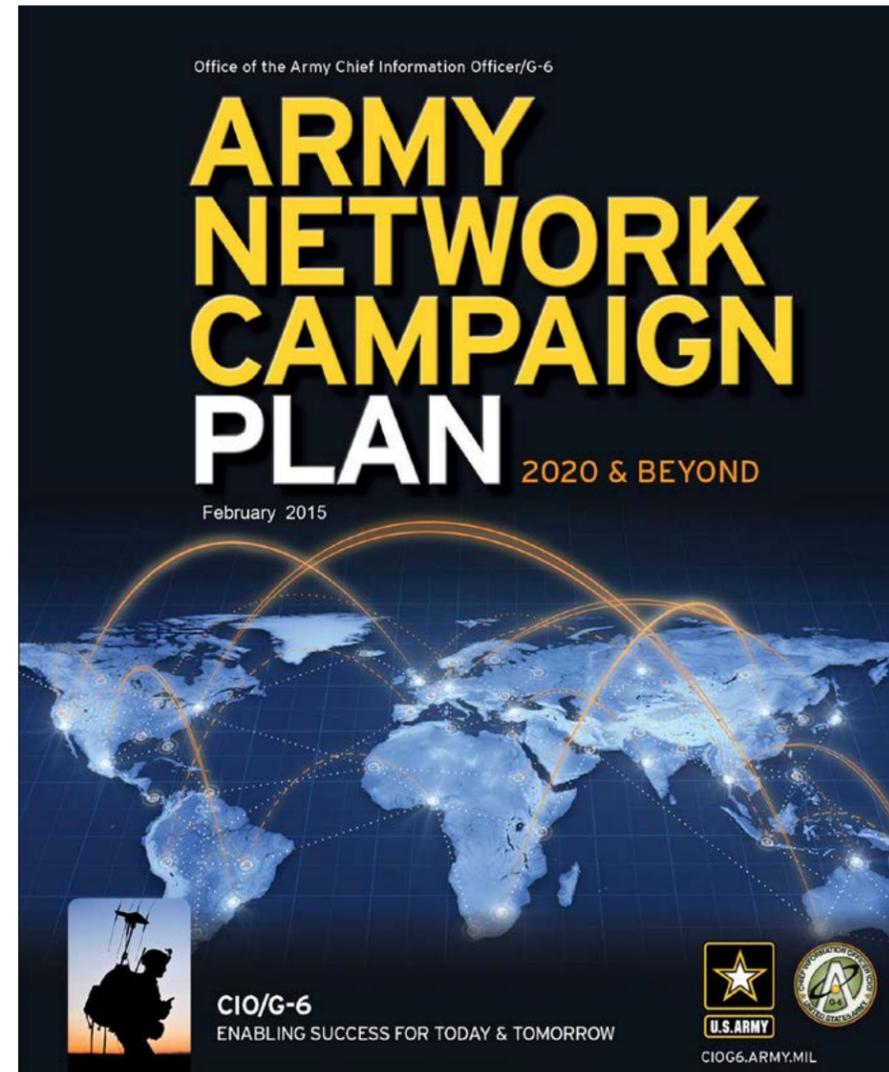
From a user perspective, it may seem as if the Army has not one but many networks: the one you use in garrison, one for the field and still another while deployed. There are differences in the look, feel and functionality of the network in different environments, in part, because different segments of the network have been built, operated and maintained for specific purposes by different organizations.



(Photo by J.D. Leipold)

For the Army to remain the most dominant land force in the world, this perceived and real fragmentation must be eliminated. In its place, the Army is now building one enterprise network

that extends across echelons, classification levels and mission environments, serves both the operating and generating forces, and enables users to connect and share information worldwide.



## Driving LandWarNet Change

The future security environment, described in the new Army Operating Concept, is characterized by uncertainty – of mission, location, timing, whom the Army will fight and with whom it will team to accomplish the mission. Deployments often will occur with little or no notice, and will entail the full range of operations, to include armed conflict, U.S. and partner training, and humanitarian assistance. Units will be geographically dispersed but expected to operate as if they were co-located. To make the force more agile and reduce logistics requirements, certain functions may remain outside the area of operations.

For the Army to succeed in these conditions, the same set of network capabilities must be accessible at home station, in the

(Continued on page 4)

(Continued from page 3)

training environment, while en route to the theater and in every corner of the AO. The network must perform reliably regardless of the physical location – from the most densely populated urban center to the most remote, most austere landscape. And, it must enable interoperability with all mission partners.

As the Army responds to changes in the operating environment by adapting the way it organizes, trains, fights and collaborates, the network must follow suit. Like any complex effort, network modernization begins with a comprehensive strategy. The Army Network Campaign Plan, with the accompanying near-term (2015-16) and mid-term (2017-21) implementation guidance, is that blueprint. It lays out how the future network will support Army 2020 and desired network end states, and sets conditions for Force 2025. Priority activities and initiatives are organized around five lines of effort. A Chief Information Officer/G-6 staff element leads each LOE to synchronize effort from the tactical edge to the enterprise and across multiple stakeholders and

communities of interest.

### 1 Providing Signal Capabilities to the Force

LOE 1 is providing Signal capabilities to the entire force. It focuses on synchronizing delivery of network capacity, security, services, training and doctrine. It also will develop a Signal equipping strategy to field intuitive, secure, standards-based capabilities that are adaptive to the commander’s requirements and integrated into the Common Operating Environment.

### 2 Enhance Cybersecurity Capabilities

LOE 2 concentrates on enhancing cybersecurity capabilities by optimizing defensive cyberspace operations and Department of Defense Information Network operations. This LOE will improve the network defense posture by minimizing the attack surface, establishing physical path diversity at critical installations, strengthening data defenses and enhancing security through cyber hygiene and best

practices. The Army intends to deploy capabilities that support cyberspace defense and enhance cyberspace situational awareness by improving the cyber-sensing infrastructure, harnessing the power of Big Data analytics and expanding information sharing.

### 3 Increase Network Throughput and Ensure Sufficient Computing Infrastructure

The third LOE centers on increasing network throughput and ensuring sufficient computing infrastructure. This LOE will generate the “always on, always available,” end-to-end transport infrastructure necessary to meet growing and evolving capacity demands. It also will shepherd the transition from disparate data processing and storage solutions to an optimized and responsive global computing and storage infrastructure. LOE 3 will implement a standardized suite of centrally managed end-user devices, as well, to improve functionality and the user experience.

### 4 Delivering Services to the Edge

LOE 4 focuses on providing capability to these devices via a universal suite of IT services, to include voice, video, data retrieval and sharing, and collaboration, from the enterprise to the edge.

### 5 Strengthening Network Operations

LOE 5 will concentrate on strengthening network operations. This includes establishing an information exchange specification framework and simplifying the design, assembly, transport and stand-up of mission-scaled networks. LOE 5 will set the requisites to enhance spectrum monitoring, assignment and de-confliction. It also will facilitate central oversight of network assets and mission readiness, creating full network situational awareness; and improve incident response and cybersecurity management services for the operating force.

The ultimate goal for these lines of effort is to produce a single, integrated information environment that is comparatively simple to operate and maintain, protected against compromise, inherently Joint and interoperable, and serves as the backbone of an agile, expeditionary, always ready Army. Common infrastructure, such as core data centers and Joint Regional Security Stacks, will support generating and operating forces, active and reserve components, and

the unique requirements of the engineer, intelligence, medical and logistics communities. Centralized hosting and storage, and cloud-based delivery, will make data, applications and services universally available to all authorized users. The approved set of computing technologies and standards known as the Common Operating Environment will open the door to rapid development and fielding of secure, plug-and-play capabilities, including more commercial off-the-shelf solutions.

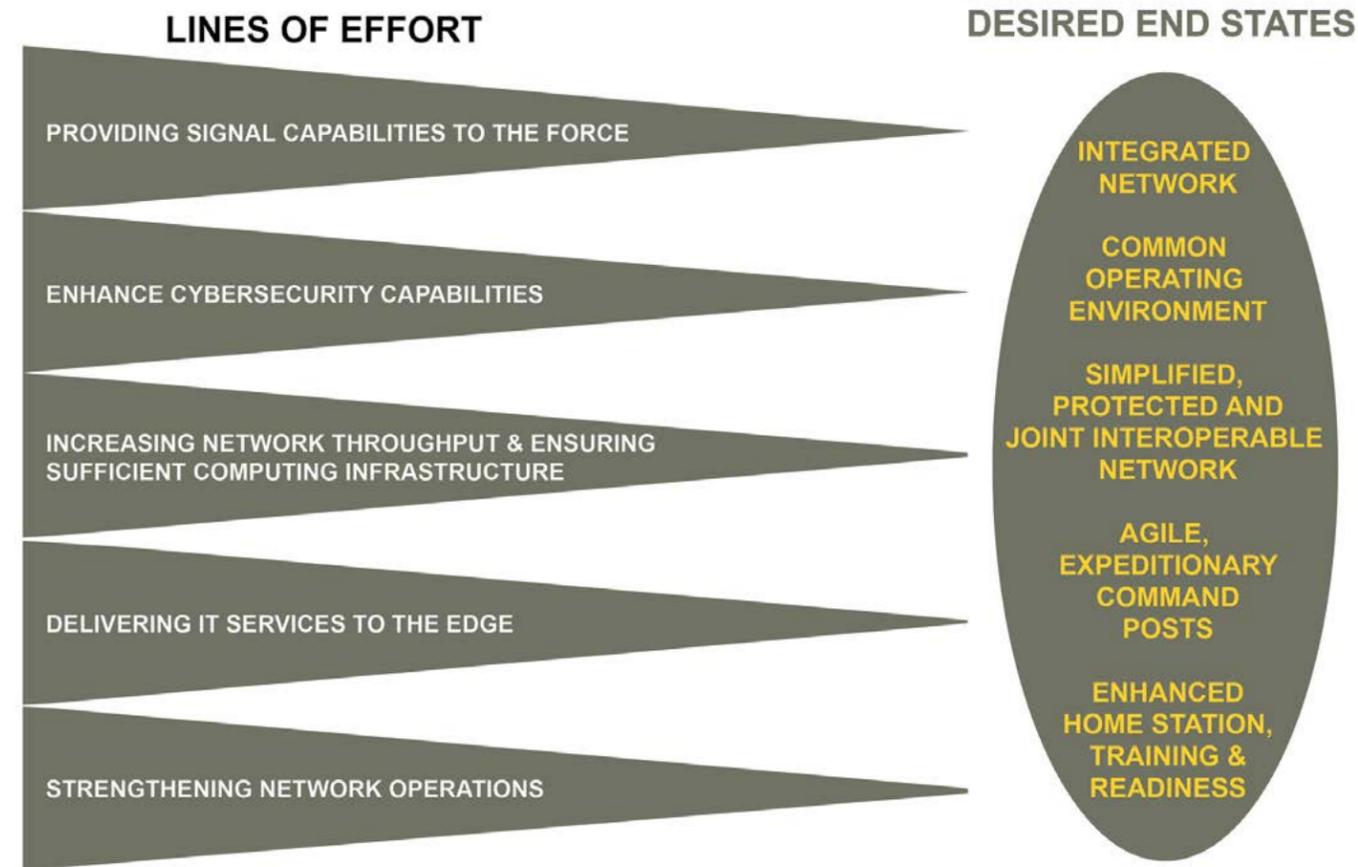
This enterprise-level modernization feeds directly into preparing and enabling our tactical units. Mission command systems and applications will remain operational in garrison at all times. When at home station, Soldiers will work with same technologies and capabilities they do in their training and operational environments – making it easier to maintain proficiency and to keep these critical systems up to date with software and security upgrades. Through Installation as a Docking Station, units will receive real-time situational awareness and understanding from forces in theater – before they deploy -- and will continue to get current information while en route. Secure mobile devices that function in all environments and can tap Army and Joint information resources and services will become commonplace. Mission command and functional applications will have the same look and feel regardless of the device running them or the user’s location.

On the ground, true distributed mission command will become a reality, making the Army more expeditionary and more effective on the battlefield. Deployable command posts will be more mobile and agile thanks to smaller, lighter network components with lower power and cooling requirements, coupled with a robust fixed network infrastructure that has the capacity and flexibility to support home-station mission command centers. Commanders will be able to continuously inform and influence their forces through every operational phase, no matter how dispersed they are. They, and Soldiers, also will be able to leverage intelligence processing, exploitation and dissemination services.

### The Challenges Ahead

Network modernization is an enormous, complex effort. Technology will continue to evolve rapidly,

(Continued on page 6)



(Continued from page 5)

with computing power – and the capabilities that consume it -- growing exponentially in ever-shorter cycles. The “Internet of Things” paradigm will encompass more and more functionality. As cutting-edge advances become available to the U.S. military, so too will potential adversaries have access. The cyberspace threat environment will morph continuously and, as the other warfighting domains became more dependent upon the network, the need for stringent security and defense will expand. At the same time, the military will continue to face an uncertain fiscal environment. Tighter budgets and the lack of financial predictability may impact the pace and depth of modernization, sustainment of equipment, and even recruiting, training and retaining talented personnel to operate, maintain and defend the network.

Keeping our warfighting edge under these conditions will require keen, strategic anticipation of Soldier needs and possible solutions, followed by agile adaptation of technology. Investments in network and information technology must yield the greatest rewards in terms of performance and benefits to the entire Joint team, and the Army must look for opportunities to share the cost of building, operating and maintaining new

capabilities with other DoD components, as aligned to the Joint Information Environment. We will have to design, develop, acquire and field IT in a comprehensive, synchronized manner that addresses critical capability gaps in an incremental, affordable fashion. As the Army gets smaller, the capabilities we select must empower leaders at the lowest levels with relevant combat information, situational understanding and access to Joint and Army capabilities, without increasing manpower requirements. Additionally, recognition and mitigation of internal vulnerabilities and external threats must become lightning-swift.

Achieving a modernized network will require a very broad team effort. CIO/G-6 is actively engaged with the Assistant Secretary of the Army (Acquisition, Logistics and Technology), Training and Doctrine Command, G-3/5/7, G-2, Second Army, Army Cyber Command, the Defense Information Systems Agency, our sister Services and industry to ensure that we capture all user needs and implement the right technologies and services to fulfill them, cost-effectively and efficiently. Insights from the field are particularly valuable; the CIO/G-6 door is wide open to the thoughts and recommendations of the Signal Regiment. Working together, we will provide the

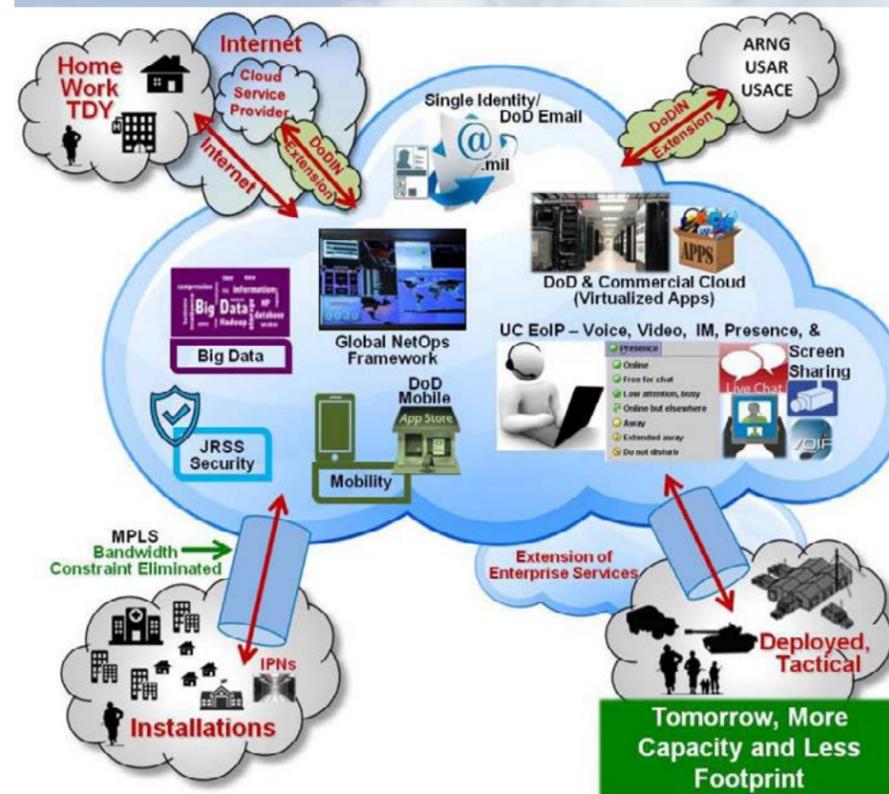
robust, end-to-end network necessary to enable the success of our Soldiers for today and tomorrow.

*LTG Robert S. Ferrell joined the Army in July 1977 and was commissioned as an officer in the Army Signal Corps in August 1983. His career has taken him throughout the United States, Europe and Korea, and he has been deployed to Bosnia and Iraq. His most recent assignments have included serving as the Director of C4 systems and Chief Information Officer for the U.S. Africa Command in Stuttgart, Germany and as Commander of the Communications-Electronics Command, known as CECOM, at Aberdeen Proving Ground, MD. LTG Ferrell became the Army Chief Information Officer/G-6 in December 2013.*

*COL Linda Jantzen was commissioned in the Army Signal Corps through the ROTC program in 1988. She has served in multiple command and staff assignments worldwide including command of the 40th ESB in Fort Huachuca, Ariz., and the 160th Signal Brigade, Camp Arifjan, Kuwait. She is currently assigned as a Division Chief in the Architecture, Operations, Networks and Space Directorate of the Army's Chief Information Officer/G-6.*

# The Cloud-enabled Network

By COL John Rozsnyai



The world is evolving into an increasingly interconnected environment. The Army of 2020 will operate in a complex world where cloud-based computers receive data from tens of billions of devices. These computers will have the capacity to digest, correlate, contextualize, process and then present data back to humans in a way that assists our decision-making process. The Army is modernizing its network to prepare for the impending data-driven, cloud-based world as depicted in the figure above.

Cloud technology is crucial to giving the Army, and ultimately the Joint team the information environment, the universal availability, expansive capacity and stringent security the U.S. Army operating concept demands.

## ACRONYM QuickScan

AO – area of operations  
ANCP – Army Network Campaign Plan  
CIO – Chief Information Officer

DoD – Department of Defense  
LOEs – Lines of Effort

(Continued from page 7)

With the third decade of the 21st century closing in, uncertainty and volatility have become the dominant factors in the global threat environment. The things we can count on are few and, in their own ways, often open the door to even more unknowns. Taking today as a benchmark, we can be certain that U.S. forces will remain in high demand around the world – though we can't predict exactly where and in what circumstances -- and the Army's operational tempo won't change much. We will continue to work in Joint, coalition and inter-agency settings. Our adversaries will become more sophisticated and their access to cutting-edge technology, especially information technology, will get easier. The threat to DoD networks definitely will intensify. And, all of this will occur over a national financial backdrop that indicates a smaller Army and lower defense budgets.

Already, the network underpins everything the Army does and that won't change in these conditions; in fact, we'll likely become even more reliant on it. But the network's design and the way the Army employs information technology capabilities must be revamped. To make the force truly expeditionary, the network must have a very specific set of characteristics: worldwide reach, whether at home station, en route, just entering the area of operations or in a mature theater; guaranteed availability, regardless of location and the number of users; and a level of security that protects the integrity of the network itself and the data it carries. The bottom-line requirement is to provide all authorized personnel access to the information, services and capabilities they need, anytime, anywhere.

Cloud technology will help make this robust, versatile network a reality. Its key elements will be crucial to giving the Army, and ultimately the Joint team via the Joint Information Environment, the universal availability, expansive capacity and stringent security the U.S. Army operating concept demands. By pooling configurable computing resources, such as servers, storage, applications and services, the cloud model creates elasticity and responsiveness. Computing resources appear unlimited to the user; however, they can be monitored, reported and automatically controlled and optimized through a metering capability (tied,

for instance, to storage, processing, bandwidth and active user accounts), quickly scaling up or down commensurate with demand. Authorized users can rapidly provision and release services, with minimal management effort or service provider interaction, producing an on-demand, self-service type of environment. The cloud also enables device-agnostic access to capabilities and services, making the switch from mobile phones to tablets to laptops and workstations seamless for the user.

### What the Cloud Brings to the Table

The most important aspect of the cloud is the power it gives Soldiers and leaders. Cloud capabilities will assure that computing and communications resources, authoritative data sources and services are available, accessible and safeguarded -- from the highest levels of the enterprise to its tactical edge. As the network aggregates, processes and presents data in a way that is easily understood, Soldiers will be able to make informed, more effective mission decisions. Moreover, commanders, senior leaders, decision makers and even mission partners will be able to reach and correlate larger quantities of data, customize those data to fulfill their needs and objectives, and share those data and their operational insights. When coupled with the appropriate applications and a common data structure across the Army and DoD, the cloud also will allow users to harness the potential of Big Data analytics.

Beyond the tactical arena, a cloud-enabled infrastructure will support faster implementation of new systems and capabilities, which will become available to everyone at the same time – rather than over months or even years due to staggered, localized fielding. Further, with upgrades made seamlessly behind the scenes, the introduction of new and improved technologies, and security updates, will carry limited impact to the user. The Army's approach also will emphasize minimizing Army ownership, operation and sustainment of hardware and other commoditized information technology in favor of procuring capabilities as services from cloud providers. Over time, this and the inherent economies of scale will translate into lower costs and allow the Army to focus its limited resources more effectively on meeting mission needs.

The Army plans to leverage the cloud to advance mobility, as well. The Army will adopt commercially available mobile applications that enable the use of

cloud-hosted solutions to the maximum extent possible and, where good solutions are absent, pursue development of Army-specific mobile applications that leverage cloud computing and storage capabilities, and consciously reduce and optimize network resource usage.

Authorized end users will be able to retrieve and install approved mobile applications from the Mobile Application Store. The Army also will evaluate a cloud-enabled "bring your own device" capability to make authoritative

information more widely available to the Total Force while reducing overall costs.

### The Cloud Blueprint

Cloud capabilities require a foundation of tight security and ample throughput, both of which are primary focus areas of the Army Network Campaign Plan. They also need a clean, clutter-free environment, rendering current efforts to rationalize existing systems, applications and data even more important.

To ensure the maximum

level of interoperability across hosting environments and among Department of Defense components and mission partners, the design and use of the Army cloud will follow approved JIE, LandWarNet 2020, Army cloud architecture, Information Architecture and operational directives. But from there, the blueprint opens up. Under the Army Cloud Computing Strategy published in March, there are three potential cloud service models:

(Continued on page 10)



# Army Transition to Cloud

Strategic Cloud Imperatives	Adopt Cloud Governance & Management Practices	Instantiate Cloud Computing Capabilities within the Army Network	Managing the Mod & Migration of apps, systems & data	Secure & Manage Cloud Operations
Enabling Objectives	<ul style="list-style-type: none"> <li>• Synchronize planning, resources &amp; acquisition activities                             <ul style="list-style-type: none"> <li>• Leverage IPT for application hosting</li> <li>• Formulate resources to deploy cloud capabilities aligned with ANCP</li> <li>• Develop standard contractual terms</li> <li>• Enforce COE standards</li> <li>• Leverage AAMBO</li> </ul> </li> <li>• Develop policy &amp; processes for monitoring compliance                             <ul style="list-style-type: none"> <li>• Define Organizational R&amp;R</li> <li>• Enforce AAMBO</li> <li>• Leverage Network Capability set</li> <li>• Leverage C4IM Catalogue Management Process</li> </ul> </li> <li>• Develop integrated architectures                             <ul style="list-style-type: none"> <li>• Develop technical &amp; solution architectures</li> <li>• Dev &amp; Implement Army enterprise service manage</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>• Increase network throughput                             <ul style="list-style-type: none"> <li>• Upgrade installation infrastructure</li> <li>• Complete MPLS core transport &amp; other transport mod upgrades</li> </ul> </li> <li>• Id &amp; leverage appropriate cloud models                             <ul style="list-style-type: none"> <li>• Leverage Designate DAA R&amp;R</li> <li>• Define Common Service Support</li> <li>• Conduct centrally controlled pilots</li> <li>• Leverage gov't &amp; commercial cloud hosting (IaaS/PaaS/SaaS)</li> <li>• Develop a catalog of existing infrastructure, application, &amp; data services</li> </ul> </li> <li>• Integrate secure mobile computing capabilities                             <ul style="list-style-type: none"> <li>• Est Software Mkt Place</li> <li>• Leverage Enterprise mobile Device Mgt</li> <li>• Eval BYOD capability</li> <li>• Ensure STIG/SRG controls</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>• Maintain single AAMBO                             <ul style="list-style-type: none"> <li>• Negotiate &amp; acquire cloud capabilities from CSP's</li> <li>• Facilitate the transition of user IT services from local implementations to enterprise capabilities</li> </ul> </li> <li>• Modernize applications to conform &amp; operate within a cloud environment                             <ul style="list-style-type: none"> <li>• Ensure data is in accord. with Army Data Strategy.</li> <li>• Properly categorize applications &amp; data</li> <li>• Standardize computing hosting &amp; storage infrastructure</li> </ul> </li> <li>• Ensure data is in accordance with Army Information Architecture                             <ul style="list-style-type: none"> <li>• Rationalize data sources to retrieve data elements</li> <li>• Leverage the DoD data service environment registry</li> <li>• Facilitate transition to publish data exchange capabilities</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>• Ensuring security &amp; reducing risk                             <ul style="list-style-type: none"> <li>• Establish the defense-in-depth posture</li> <li>• Make access control dynamic by leveraging enterprise IdAM</li> <li>• Transfer security vulnerability &amp; patch management</li> <li>• Leverage the Big Data analytic environment</li> <li>• Partner with CSP's FedRAMP &amp; DISA for approval &amp; compliance</li> </ul> </li> <li>• Develop standards for acquiring &amp; managing cloud operations                             <ul style="list-style-type: none"> <li>• Develop CONOPS for operation &amp; management of applications</li> <li>• Develop standard contractual terms, conditions, &amp; SLA's</li> <li>• Integrate Army computer network defense service provider function into CSP's</li> </ul> </li> </ul>
Alignment to ANCP LOEs	LOE 1 – Provide Signal Capabilities to the force LOE 5 – Strengthen Network Operations (NetOps)	LOE 3 – Increase Network Throughput and Ensure Sufficient Computing Infrastructure LOE 4 – Extend Enterprise Services to the Edge	LOE 3 – Increase Network Throughput and Ensure Infrastructure LOE 4 – Extend Enterprise Services to the Edge LOE 5 – Strengthen Network Operations (NetOps)	LOE 2 – Enhance Cybersecurity Capabilities LOE 5 - Strengthen Network Operations (NetOps)

(Continued from page 9)

infrastructure as a service, platform as a service, and software as a service. [could insert graphic here]

There also will be multiple options for the cloud deployment model: private, community, public and hybrid. For the Army, the deployment model is important due to DoD cybersecurity requirements and legal limitations regarding where DoD data can be hosted. The Army will use the DoD Risk Management Framework, the special considerations outlined in NIST 800-144, the various levels of data sensitivity described in DoD Cloud Computing Security Requirements Guide and the mission criticality of the system or application to determine which model is appropriate. For example, the Army would evaluate off-premises commercial cloud offerings for data impact levels 1 through 5. However, when an application processes classified data (Secret and above), the Army will look for private cloud infrastructure, either in its own facilities or other certified DoD facilities. The Army also will deploy local cloud instantiations, when necessary, to support critical operational needs.

The Army intends to rapidly capitalize on Federal Risk and Authorization Management Program and DoD-approved government and commercial cloud service providers to the extent that doing so aligns with mission requirements and does not compromise security. This should reduce the amount of contracting and cybersecurity resources required, shorten implementation timelines, and more effectively keep pace with emerging technologies.

A cloud-based network demands dynamic security – that is, continuous monitoring and evaluation of systems, capabilities, interfaces, applications and data transactions to assess threats (external and insider) and risks that may affect confidentiality, integrity and availability.

Security countermeasures will be integrated from the beginning, protecting each element of data, tracking provenance and matching each user's roles and authorizations against each data security label to ensure proper access only.

Provenance will enable auditing and real-time forensic analysis to identify all users, products and processes that used the data; to protect against cyber

attack; and to respond following any unauthorized disclosure of information.

Venturing into the world of commercial cloud service providers will require different and faster acquisition, contracting and IT accreditation processes. Service level agreements must enforce the use of Army and DoD data standards and ensure application interoperability, data and application portability between providers (to preserve the Army's ability to change vendors in the future) and the eventual removal of data from infrastructure. In addition, the Army will have to carefully test and evaluate ahead of contracting actions, with an eye on obtaining agnostic solutions and avoiding platforms and technologies that lock customers into a particular product.

### Cloud constraints

While a cloud-based architecture holds enormous potential, it will not be suitable for every network and IT requirement. First and foremost, the Army must ensure that it does not compromise its mission by unrealistically trading the confidentiality, integrity and availability of critical data and information in pursuit of the benefits the cloud may offer. In particular, the potential vulnerabilities of and impacts to expeditionary operations must be continuously assessed and weighed against the advantages of adopting cloud technologies. The Army must carefully consider the effects on mission command during en route mission planning, forces operating in highly contested and disconnected, intermittent or low-bandwidth environments as well as cybersecurity and legal boundaries. However the Army designs and employs the cloud, it must allow individuals and units to disconnect from the network; continue to conduct operations and create and process mission-critical data locally; then reconnect and resynchronize with the network as connectivity is restored.

Application and system migration decisions must take into account the risk to the mission posed by loss of access to, or compromised integrity or confidentiality of, information. The Army also must ensure that data classification levels are not compromised due to aggregation of data. The cloud architecture must not increase technical complexity,



lead to system performance issues or outages, or amplify vulnerability to attack. Additionally, it must be able to accommodate the competitive, congested and contested cyber-electromagnetic environment the Army expects.

### Looking Ahead

The potential of the cloud to improve overall capability is indisputable. Yet, incorporating the cloud into combat and other operations presents uncharted territory. The Army will proceed with due caution, integrating cloud-enabled capabilities incrementally to ensure that our own warfighting effectiveness and our ability to operate and collaborate with mission partners are not eroded. Candid input from the field throughout adoption will be critical to gauging the impact – positive and negative – of the cloud-enabled network. The Chief

Information Officer/G-6 is counting on the Signal community to help determine what works, and what doesn't.

*COL John Rozsnyai is a native of South Carolina and has served in the U. S. Armed Forces since 1988. Some of his previous assignments include serving as the Chief, Information Technology Policy and Governance Branch, National Guard Bureau and Current Operations Officer and Military Deputy to the Director, Capability Development and Integration Directorate, U.S. Army Cyber Center of Excellence at Fort Gordon, Ga. COL Rozsnyai is currently assigned at Headquarters, Department of the Army Chief Information Officer/G-6, as the Chief, Enterprise Architecture Division, Army Architecture Integration Center, Architecture, Operations, Space, and Networks Directorate.*

### ACRONYM QuickScan

**DoD** - Department of Defense

**ESB** - Expeditionary Signal Battalion

**FedRAMP** - Federal Risk and Authorization Management Program

**NCW** - Network Centric Waveform

**NetOps** - Network Operations

**NIPR** - Non-secure Internet Protocol Router

# No longer a dream in the cloud

*Joint Base San Antonio Team Conducts Huge Network Infrastructure Modernization*

*By Dennis Garrison*

The Army and Air Force achieved a major network security and capacity upgrade at Joint Base San Antonio in partnership with the Defense Information Systems Agency.

This is the first Department of Defense location to achieve the pairing of new switching technologies and security stacks.

On-line traffic for both JBSA-Fort Sam Houston and JBSA-Lackland now flow through a new Joint Regional Security Stack. In addition, network speed for end users has increased dramatically.

This is a tremendous step in terms of transitioning to a joint security architecture and making the joint information environment a reality. It also speaks to successful teaming by the Army, DISA, Air Force and the Army's initial investment in this new joint capability.

New JRSSs will cut DoD-wide top-level security stacks from about 1,000 worldwide to 50. This means the cyber perimeter becomes more defensible.

"The JRSS Management Suite allows us to monitor and centrally control our security configurations. As new threats emerge, we can quickly assess the risk and more effectively mitigate identified risks across the enterprise," said Mark Orndorff, DISA mission assurance executive. "JRSS also lowers costs for the entire DoD."

To maximize bigger information "highways," the Army and Air Force, along with DISA, are implementing Multi-Protocol Label Switching, a virtual traffic management system that moves data faster, improves command and control, and prioritizes and smoothes data flow; the chances of



data being stalled or lost due to high volume and congestion are greatly reduced. This year, MPLS-supported routers are being installed at 22 locations. DISA plans to finish implementation for a total of 90 sites, by September 2015. MPLS upgrades also help set the conditions to deliver enterprise services from the enterprise to installations and the tactical edge.

Current DISA and Army efforts will increase network backbone bandwidth more than ten-fold to 100 gigabits per second (gbps) and individual Army installation capacity will increase dramatically as well.

The Army is replacing all aging building switches at nine Army installations with 11,000 ethernet switches capable of providing 10 gbps.

Lessons learned at JBSA will inform full-scale implementation across the continental United States and around the world. Short-term targets include refining network upgrades at Wiesbaden, Germany, and installing two JRSS in Southwest Asia.

## ACRONYM QuickScan

**DISA** - Defense Information Systems Agency  
**JBSA** - Joint Base San Antonio

**JRSS** - Joint Regional Security Stack  
**MPLS** - Multi-Protocol Labael Switching

# Command Post of the Future evolves web-based capabilities

*By Kathryn Bailey*

With more than 20,000 systems deployed or in use around the world, the Army's collaborative support system has begun a three-phased approach that will sustain its current capabilities and then transition into a collaborative web environment that reaches across all echelons - and all devices.

This system, the Command Post of the Future processes and displays combat information onto digital maps from other Army systems at the battalion and above echelons, including from the Joint Battle Command-Platform, which allows Soldiers in vehicles to track friendly (blue) and enemy (red) forces, and the Advanced Field Artillery Tactical Data System, used for comprehensive fire support capabilities.

"CPOF revolutionized the face of the command post," said COL Michael Thurston, project manager for mission command. "It produced the technological leap from acetate maps to digital screens, and became the foundation for the advanced, collaborative technologies our Soldiers are using now or soon will be."

These advanced technologies are part of the Army's Command Post Computing Environment



**The Command Post of the Future continues making enhancements to its map-based, situational awareness capabilities as a tactical applications suite designed to merge and simplify command post technologies within a web environment.**

and Mounted Computing Environment, which consolidates capabilities using web-based apps and displays them on a common, geospatial digital map hosted on a single workstation or mobile device.

Beginning in FY 2015, all earlier versions of CPOF up to 10.0 will move to the sustainment phase with the Software Engineering Center at Aberdeen Proving Ground. The SEC, part of the Communications-Electronics Command, provides software support services to the command, control, communications, computers, intelligence, surveillance and reconnaissance community. One of the more recent and critical enhancements to CPOF is the Disconnected, Intermittent, Limited function. DIL

capabilities provide uninterrupted operations in the event of a network outage or the requirement to rapidly relocate a command post by allowing individuals and units to disconnect from the network, continue to conduct mission command operations using CPOF, and then reconnect and resynchronize with the data repository.

By FY 2019, CPOF functionality will transition to a web application-based solution set, tentatively termed Tactical Applications. TacApps is TMC's portion of CP CE (v3), and will merge several mission command capabilities onto one. In addition to CPOF, TacApps will include Command Web, the framework that supports web-app development; Battle Command Sustainment and Support System, which includes all of the logistics web apps; and Common Tactical Vision, an up-and-coming situational awareness capability that includes a DVR-like playback function.

Within TacApps is an application infrastructure, also evaluated at NIE 15.1, that will allow seamless collaboration and a shared understanding - not just across different systems - but across echelons to address the Army's shared workspace initiative.

## ACRONYM QuickScan

**AFATDS** - Advanced Field Artillery Tactical Data System  
**APG** - Aberdeen Proving Ground  
**BCS3** - Battle Command Sustainment and Support System  
**C4ISR** - Command, Control, Communications, Computers, Intelligence Surveillance and Reconnaissance  
**CP CE** - Command Post Computing Environment

**CPOF** - Command Post of the Future  
**CTV** - Common Tactical Vision  
**DIL** - Disconnected, Intermittent Limited  
**JBC-P** - Joint Battle Command-Platform  
**MCE** - Mounted Computing Environment  
**PM MC** - Project Manager for Mission Command  
**SEC** - Software Engineering Center  
**TacApps** - Tactical Applications

# USCENTCOM outlook

By BG Peter A. Gallagher

*The United States Central Command, along with our service components, combined joint task forces and mission partners, face a multitude of complex challenges across a volatile area of responsibility. Some complexities are a result of evolving global and regional conflicts and confrontations. Others derive from fiscal uncertainty and the Department of Defense's modernization efforts to improve the efficiency, cybersecurity and resiliency of our networks.*



Within this context, applying discipline is critical to acquiring, operating, defending, and governing the Command, Control, Communications, Computers and Coalition enterprise to provide the Combatant Commander with uninterrupted mission command to enable success at all levels and ensure the best use of limited resources.

## Strategic Environment

Throughout this dynamic Central Region, USCENTCOM remains ready, engaged, and vigilant to effectively carry out our strategic objectives and protect America's vital interests. The USCENTCOM Commander's focus is managing the current conflicts and preventing ongoing regional confrontations from escalating to conflict, while effectively shaping the underlying situations by proactive engagement to influence behaviors, perceptions and outcomes.

These ongoing conflicts, confrontations, and situations result in an extremely complicated and unpredictable operational environment.

USCENTCOM requires a resilient and flexible infrastructure throughout the AOR to support current and future operations and an always-on, ready capability to support uninterrupted mission command. In an era of political change and fiscal restraint, we must ensure proper prioritization and resourcing of activities to meet strategic end states in support of the combatant commander.

Ongoing conflicts, confrontations, and situations in the USCENTCOM AOR result in an extremely complicated and unpredictable operational environment. USCENTCOM requires a resilient and flexible infrastructure throughout the AOR to support current and future operations, and an always-on, ready capability to support uninterrupted mission command.

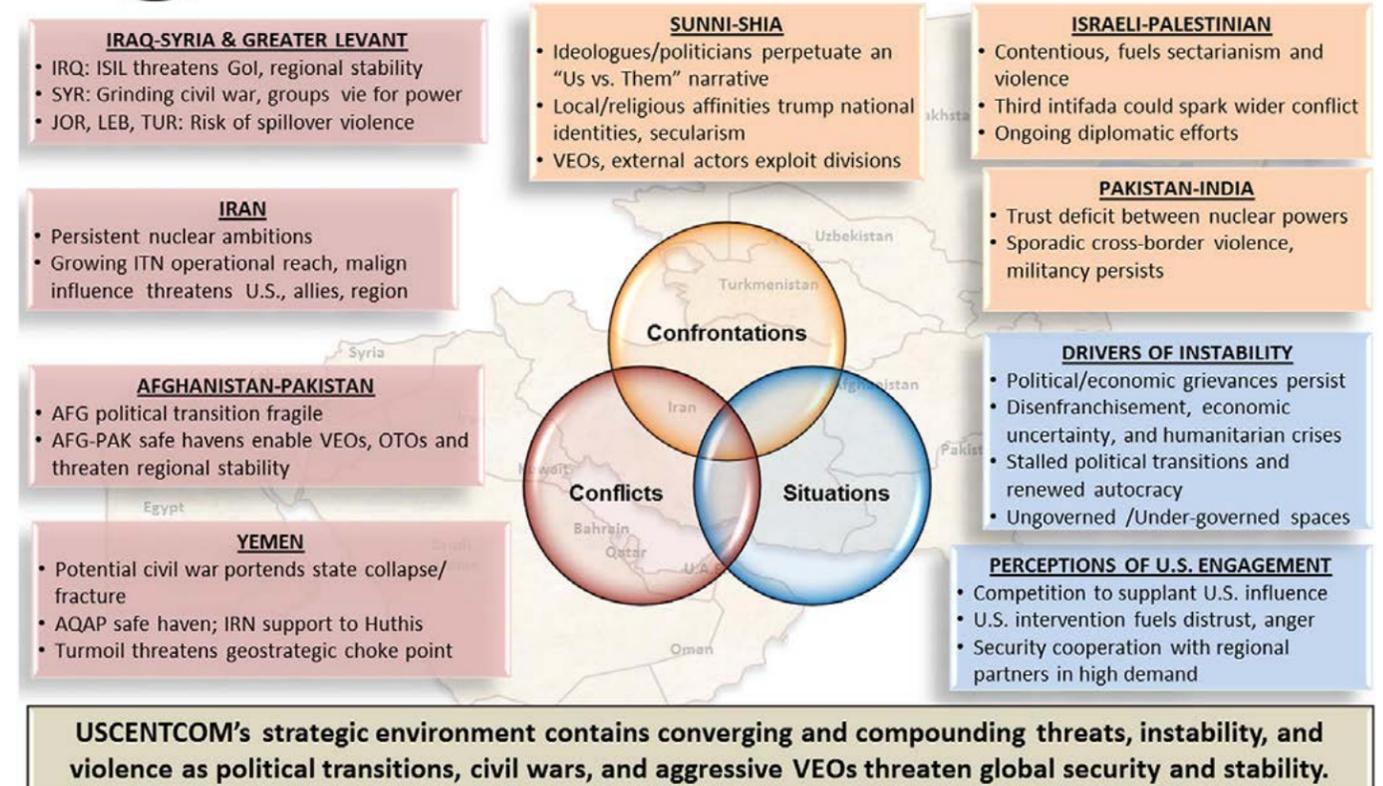
## Fiscal Environment

Over the last 14 years of war, we built a resilient headquarters and theater architecture that is

(Continued on page 16)



## USCENTCOM Strategic Environment



(Continued from page 15)

potentially at risk in a fiscal environment that demands restraint and expects good stewardship of resources. Funding for USCENTCOM programs, operations and activities is almost exclusively through Overseas Contingency Operations appropriations. The risk of this funding strategy has the potential to disrupt a diverse and survivable infrastructure essential to support operations in the USCENTCOM AOR. Budget pressures and force reductions could also influence the posture of Signal forces in this theater. The only permanently assigned Army unit in the AOR is the 160th Signal Brigade, which includes the Southwest Asia Cyber Center. The capabilities delivered by these organizations are critical to USCENTCOM's ability to execute ongoing combat operations, to sustain readiness and operate a flexible network to support commanders at all echelons.

### DoD Initiatives

The Joint Information Environment will change how DoD installs, operates and maintains Information Technology networks. Key considerations to implementing JIE in the USCENTCOM AOR are the synchronization of the Services' initiatives and efforts to deploy enterprise and theater services to strategic, operational, and tactical locations. As these efforts gain momentum, we must collaborate to achieve synergies at the regional level.

Thus far, we have done well supporting the Joint fight and delivering interoperable service-centric capabilities. The next step in this progression is to focus on design and implementation of capabilities interoperable with coalition partners.

In 2010, we implemented and expanded the Combined Enterprise Regional Information Exchange System – International Security Assistance Forces, the U.S. mission network contribution to the Afghanistan Mission Network, as a means to fight as a connected coalition. In the current strategic environment, we must integrate, share information, and exercise mission command of coalition forces on demand during Phase 0 Shaping operations. We must continue to sustain CENTRIXS-ISAF and AMN like capabilities to meet the requirement of enabling interoperability for the joint force commanders while sharing the

burden of operating and maintaining coalition networks with our partners.

### Strategic Outlook Imperative

This complex operating environment demands a deliberate and disciplined approach of governing the USCENTCOM C5 enterprise that enables mission command at all levels, while ensuring best use of limited resources. To that end, we developed a C5 Intelligence, Surveillance, and Reconnaissance Strategic Outlook aligning efforts in support of the Commander and synchronizing with DoD initiatives to achieve financial efficiencies, and improve support to ongoing operations.

The C5ISR Strategic Outlook document, referred to as our USCENTCOM J6 "Big Rocks," focuses on four lines of effort to meet strategic guidance: Optimize Theater Command, Control, Communications, Computers and Coalition, Intelligence, Surveillance and Reconnaissance Environment, Capabilities and Mission Command; Dominate Cyberspace in the USCENTCOM Area of Operations; Build USCENTCOM Partner Capacity; and Govern the USCENTCOM C5ISR Enterprise. Programs, projects and strategic initiatives in the C5 Strategic Outlook are those considered key to moving the Command and its C5 capabilities forward, and to realizing the Commander's theater vision while meeting DoD's objectives for the JIE.

### Optimizing Theater Infrastructure

Our number one priority is to provide the Combatant Commander an effective mission command platform for rapid engagement in no-notice conflicts with a connected coalition through an enduring secure mission partner environment.

Infrastructure initiatives in the Strategic Outlook focus on C5 capability effectiveness, efficiencies and security. Modernization initiatives will improve theater bandwidth availability and utilization, collapse network boundaries for improved security, and provide better command and control, all at a lower cost. The Joint Regional Security Stacks is a first step and key component of DoD's JIE providing the ability to deliver secure joint capabilities to the tactical edge. USCENTCOM will realize efficiencies through migration of coalition transport to a permanent, defensible Common Mission Network Transport and by implementing the enterprise Black Core Network at all tiers. Mobility initiatives also

focus on efficiencies, including wired and wireless Warfighter access to enterprise data assets. Key supporting initiatives include migrating to Defense Enterprise Email, Enterprise Directory Services, Core Data Center, an Enterprise Service Desk and an Enterprise Operations Center. We are making progress in planning and implementing these enterprise capabilities in our headquarters. Our alignment with Services' initiatives will allow us to achieve the efficiency, effectiveness and security goals of JIE.

### Dominating Cyberspace

USCENTCOM must be effectively postured and have sufficient capability to counter the growing cyber threat that the Nation and our regional partners now face. Maintaining an effective cyber defense posture requires the collective efforts of partners who share a common vision and are mutually committed to assured cyberspace dominance.

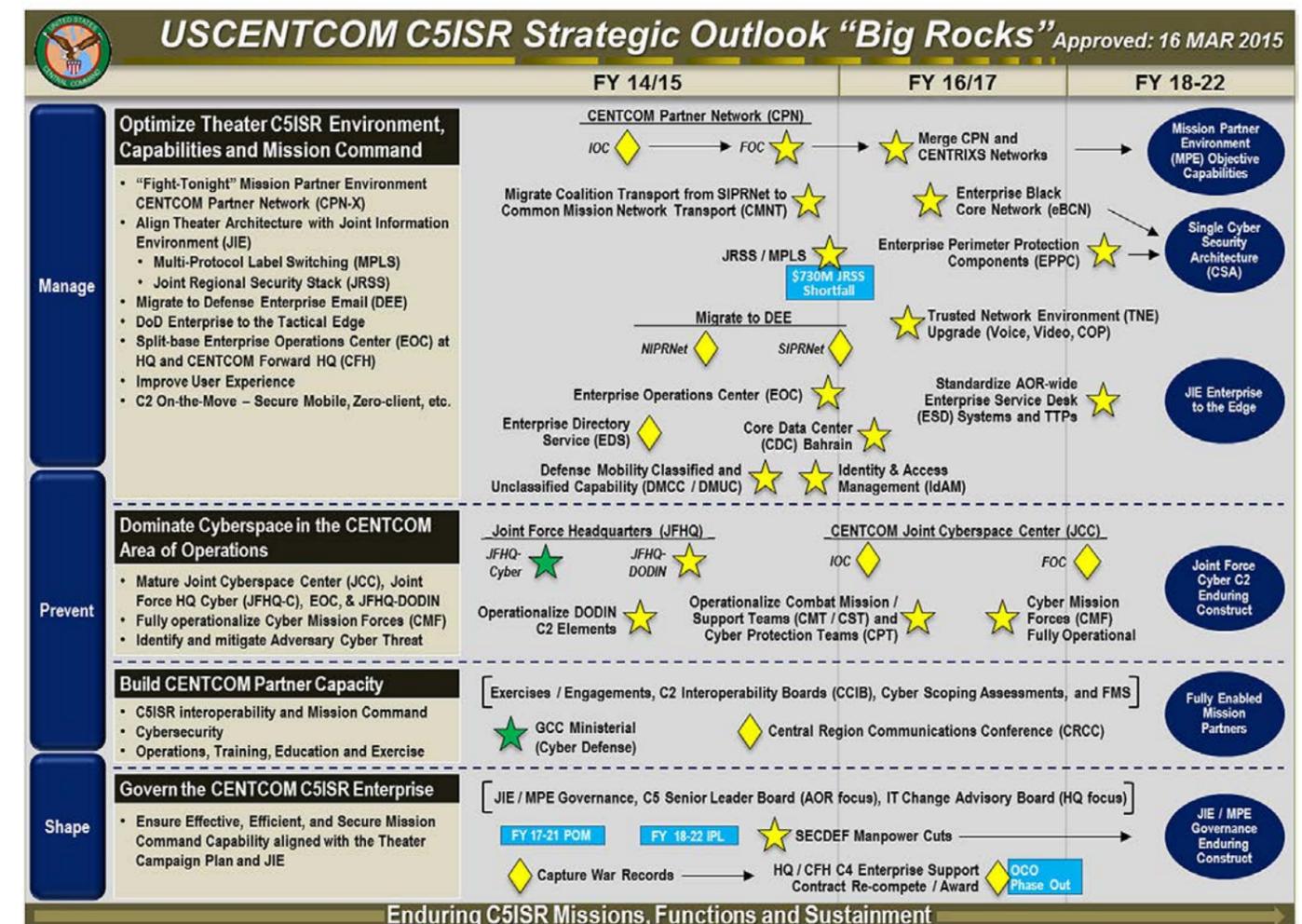
The Strategic Outlook reflects efforts to

operationalize and professionalize joint full-spectrum cyber capabilities. Army Cyber and the Joint Forces Headquarters – Cyber in Fort Gordon are key partners in this effort.

We are implementing DoD Information Network operations with our Defense Information Systems Agency Central Theater Network Operations Center and the JFHQ-DODIN construct. ARCYBER is building and aligning Cyber Mission Forces in support of the USCENTCOM Commander's priorities. The CMFs, aligned with USCENTCOM and our Service Components, are making significant contributions to the readiness of critical assets and infrastructure. Our USCENTCOM Joint Cyber Center is working diligently with U.S. Cyber Command and key stakeholders to streamline the Cyber Command and Control model in support of full-spectrum Cyberspace operations.

Looking ahead, we will focus on aggressively

(Continued on page 18)



(Continued from page 17)

improving our cyber posture to mitigate advanced persistent threats to USCENTCOM and DoD networks and critical information. As the cyber community matures, we will integrate, synchronize, and conduct cyber operations in cooperation with other US Government agencies and partner nations. USCENTCOM's cyber activities in support of regional efforts require active pursuit of solutions for key requirements including resourcing and training of cyber forces, acquisition of cyber tools and capabilities, and implementation of a command and control model aligned to the operational chain of command to synchronize orders and execution of cyber operations.

### Building Partner Capacity

Enabling USCENTCOM regional partners is a key factor in USCENTCOM mission success. To better enable coalition-operating capabilities and improve information sharing, the Strategic Outlook includes efforts to enhance partnership capacity by implementing a Mission Partner Environment. This environment combines an enduring CENTCOM Partner Network, or CPN, with an episodic Partner Network referred to as CPN-X, collectively enabling information sharing throughout all phases of an operation.

CPN-X provides commanders at the CJTF level and below the flexibility to use a federation of information sharing and mission partner networks to



(Photo by CPL Cansin P. Hardyegritag)

U.S. Soldiers from the 4th Infantry 82nd Airborne Division and Danish security adviser Overserjent Kasper inspect a malfunctioning mortar round for the Iraqi Security Forces on Al-Asad Airbase, Iraq, 10 April 2015.

exercise mission command at the operational and tactical level. CPN is a multiyear effort that resulted in the deployment of seven bi-lateral networks with critical regional partner nations in our AOR. This effort is setting the stage for an enduring MPE for DoD that can expand, collapse as required to support information sharing, and mission command of coalition operations.

USCENTCOM is collaborating closely with U.S. Pacific Command, U.S. European Command, U.S. Africa Command, and U.S. Special Operations Command to ensure every capital investment made in support of CPN is setting the stage for a global MPE solution. We have positive momentum to operationalize an enduring MPE capability with the ability to manage episodic coalition communities of interest by the end of 2016.

This requires smart decisions to capitalize on investment of OCO and program resources, common standards, the combined effort of these five Combatant Commands and the support of the DoD Chief Information Officer, Joint Staff J6, the Services, other agencies and mission partners. Collectively, we are making great strides to realize this objective.

Strategic efforts to Build Partner Capacity increase security across the AOR and focus largely on coalition exercises and engagement with key leaders and subject matter experts. The annual USCENTCOM-hosted Central Region Communications Conference is a whole-of-government, multi-stakeholder, multilateral senior leader event to address common cybersecurity



(Photo by CPL Sean Searfus)

U.S. Army MG Rick Mattson, director of exercises and training, U.S. Central Command, greets Jordanian Armed Forces soldiers and U.S. Marines with Command Element Marine Forces Central Command Forward during a visit at Camp Titin, near Aqaba, Jordan, during Exercise Eager Lion, 6 May 2015. Eager Lion is a recurring, multinational exercise designed to strengthen military-to-military relationships, increase interoperability between partner nations, and enhance regional security and stability.

and IT challenges. In addition, Cyber Security Assessments assist regional partners in building their capacity and expertise in the cyber domain.

These assessments support sharing of best practices and tactics, techniques and procedures in order to improve the ability of key stakeholders to protect in-region resources critical to the regional and global economy. Continued focus on cyber defense and cyber security cooperation supports the commander's objective to enable our regional partners to assume a greater share of the burden in providing for their own protection and will be a key component of our theater strategy.

Denmark is one of several countries participating in the U.S. led Combined Joint Task Force-Operation Inherent Resolve's Building Partner Capacity mission, which aims to increase the military proficiency of Iraqi Security Forces fighting the Islamic State of Iraq and the Levant through four to six-week periods of instruction at five different sites in Iraq. Training focuses

on small unit leadership, medical procedures, air-ground integration, and equipping and sustainment processes.

### Governing the C5 Enterprise

In USCENTCOM, we are committed to effective IT governance to ensure good stewardship of resources, compliance with DoD standards and a disciplined approach to securing and protecting networks. Good governance and stewardship of the C5 Enterprise allows us to capitalize on IT investments and re-purpose resources to set the theater and respond to contingencies. This is critical in this volatile AOR, especially with an uncertain fiscal environment.

Governing the C5 enterprise is an overarching line of effort that supports key activities and initiatives in our strategy. It synchronizes regional efforts with DoD CIO, Joint Staff J6, the Services,

(Continued on page 20)

(Continued from page 19)

other agencies and mission partners to establish a governing framework for the DoD enterprise in which we can perform our due diligence to meet mission requirements and provide a secure network given our collective fiscal constraints

### Conclusion

The current operating environment is complex with challenges that cut across multiple Combatant Command areas of responsibility. Our modernization and drive to reduce costs cannot disrupt ongoing operations in the volatile USCENTCOM AOR. Our Commanders and deployed troops deserve uninterrupted mission command and the very best network we can deliver.

At USCENTCOM, we are synchronizing the demand for fiscal restraint and transition to the JIE with the USCENTCOM Commander's Theater Campaign Plan and Priorities. We identified our J6 priorities in our four lines of effort across the Program Objective Memorandum resourcing cycle. We identified the activities and initiatives to shape, influence, and align our enduring support for Command and DoD priorities and our ability to achieve the objective end-states in the shortest timeframe possible.

The Army Signal Corps is providing unparalleled support to multiple named operations, Joint and Combined Exercises,

and Security Cooperation efforts across the USCENTCOM AOR.

In this uncertain and volatile AOR, we have not seen the end of conflict and the next crisis is right around the corner. The Army Signal Corps will continue carrying the heavy load in dealing with this uncertain future and balancing the competing demands for resources against the requirements to modernize our joint and coalition capabilities. As communicators, we must collectively find a way to provide the most creative solutions to the most complex problems.

The problems our nation faces in the USCENTCOM AOR pose a significant threat to our vital interests and way of life. If not managed within the AOR, these conflicts will follow us home.

*BG Peter A. Gallagher serves as the director of Command and Control, Communications and Computer Systems, J6 U.S. Central Command, MacDill Air Force Base, Fla. He is responsible for the implementation and management of the global communications and computer networks for the U.S. Central Command. BG Gallagher was commissioned as a distinguished military graduate from the Reserve Officer Training Corps program at Pittsburg State University in 1986. His military career includes a variety of positions providing communications support to Infantry Divisions and Special Operations Forces throughout the world. He commanded Soldiers at the platoon, company troop, battalion, squadron and brigade levels.*

### ACRONYM QuickScan

**AMN** - Afghanistan Mission Network  
**AOR** - Area of Responsibility  
**ARCYBER** - U.S. Army Cyber  
**C5** - Command, Control, Communications, Computers and Coalition  
**C5ISR** - Command, Control, Communications, Computers and Coalition, Intelligence, Surveillance and Reconnaissance  
**CENTRIXS-ISAF** - Combined Enterprise Regional Information

Exchange System - International Security Assistance Forces  
**CIO** - Chief Information Officer  
**CJTF** - Combined Joint Task Force  
**CMF** - Cyber Mission Forces  
**CPN** - CENTCOM Partner Network  
**CPN-X** - CENTCOM Partner Network Episodic  
**DoD** - Department of Defense  
**DODIN** - Department of Defense Information Network

**IT** - Information Technology  
**JIE** - Joint Information Environment  
**JFHQ** - Joint Forces Headquarters  
**LoE** - Line of Effort  
**MPE** - Mission Partner Environment  
**OCO** - Overseas Contingency Operations  
**USCENTCOM** - U.S. Central Command

# AFRICOM *Enabling African Partners*

By COL Patrick Dedham

*Teamwork and adaptability are the two most important attributes required for success in a geographical combatant command. At AFRICOM J6 these skills are essential given our mission to enable our African partners' success through the improvement of their command, control, communications and computer support abilities throughout the continent of Africa.*



(Photo by SSG Kevin Hinuma)

U.S. Marine Corps SSG Adam Haley, 24th Marine Expeditionary Unit joint terminal attack controller, observes a French Air Force Rafale M multi-role fighter aircraft flyby during a training exercise in Arta, Djibouti, 4 Feb 2015. The aircraft was part of a scheduled bilateral training exercise to prepare U.S. and French militaries for future joint operations.

(Continued on page 22)

(Continued from page 21)

The AFRICOM J6 team has four imperatives that guide our actions and are synchronized with the Commander's vision and intent. First, we ensure C4 system support and leadership. Second, the team within AFRICOM J6 and external to the command must defend and ensure cyber domain availability. Third, we must move the command to the Joint Information Environment. Finally, the most long-term impactful imperative for our mission is to expand and improve African partner C4 capabilities.

The African environment poses several unique challenges. The continent covers a land mass of 11.7 million square miles or roughly three times the size of the continental United States and is comprised of 54 nations, more than 800 separate ethnic groups, and over 1,000 different languages. Over 40% of its population is under the age of 15. According to the Human Development Index, the 20 lowest ranking countries are located in Africa, several of which have literacy rates below 50%. Much of the continent lacks basic public infrastructure including low Internet penetration.

While these statistics may seem insurmountable there are bright spots. Some nations have experienced double digit economic growth and increased political stability. For example, in Nigeria 71% of adults possess cellular phones, and since 2003 the growth of Africa's cellular industry has outpaced all other regions in the world.

Building upon the continent's successes while being mindful of its challenges – both physical and social – represents the landscape from which the AFRICOM J6 works to find success for our African Partner's C4 capabilities through exercises and engagements.

The command's joint and combined exercise program has created several opportunities to directly engage with our African Partners.

Additionally, it has developed a unique opportunity for African militaries to interact with neighboring countries and regional partners that otherwise would not have occurred. The Command's annual communications focused exercise, African Endeavor, has yielded a number of mutual benefits.

It exposes our African Partners to the

technologies and methodologies employed by U.S. forces while enabling us to better understand the capabilities and challenges of our partners. Through African Endeavor we continue to increase partner capacity while improving coalition interoperability.



(Photo by SSG Kevin Inuma)

French 3rd Maine Artillery Regiment members provide over watch during a bilateral close air support training exercise in Arta, Djibouti, 4 Feb 2015. The event was part of a scheduled bilateral CAS exercise between a contingent of 24th Marine Expeditionary Unit Marines and French soldiers and sailors.

Our military-to-military engagements program serves as a model for the Command and continues to expand from one event in 2011 to five in 2015. These events expose our African partners to a range of topics from cyber security to training and developing professional Signal officers and non-commissioned officers, while supporting themes such as gender mainstreaming.

Feedback from many of the attendees indicates that this exposure has directly contributed to improvements in how some African nations are training and professionalizing their Signal Corps.

Another important facet of our engagements and exercises is the J6 cyber security partnering program. The goal of this new program is to mature our African partner's cyber security so they can protect their key and critical infrastructure, safeguard sensitive information, and ensure availability of their communications and information sharing networks. The cyber security partnering program ideally begins with an assessment, either partner driven or done by AFRICOM, and it enables the team to tailor engagements and events to increase capability. AFRICOM uses many available resources from across the DoD and interagency to help improve the targeted cyber security areas for our African partners.

Finally, by combining engagements and exercises with cyber security improvement

***The AFRICOM uses many available resources from across the Department of Defense and interagency to help improve the targeted cyber security areas for our African partners.***

objectives for our African partners the AFRICOM J6 is regularly engaged with security force assistance. This includes installing bi-lateral and multi-lateral coalition networks in partner African nations for the purposes of information sharing. The AFRICOM J6 team is also heavily involved with providing robust High-Frequency radios for operational and tactical uses by our African partners. After the installation of network single-channel radio capabilities

the African partner is trained on maintenance and operations of the equipment, which provides and additional capability growing opportunity.

Expanding and improving African partner C4 capabilities while successfully executing the other AFRICOM J6 imperatives makes our teamwork and adaptability vital. Africa is both a challenging and rewarding environment for a signal professional. Working with the AFRICOM J6 African partners creates a very positive and unique experience.

*COL Patrick Dedham was commissioned in the Army Signal Corps through the ROTC program in 1988. He has served in multiple command and staff assignments worldwide including the G6 for the 82nd Airborne Division Fort Bragg N.C., CJ6 of CJTF-82/Regional Command East in Afghanistan, J6 for the International Security Assistance Force Joint Command in Afghanistan, and commander of the 11th Signal Brigade. He is currently assigned as the J6 for U.S. Africa Command in Stuttgart, Germany.*

#### ACRONYM QuickScan

**C4** - Command, Control, Communications and Computer  
**GCC** - Geographical Combatant Command  
**JIE** - Joint Information Environment  
**HF** - High Frequency  
**IJC** - International Security Assistance Force for Joint Command

# Operation United Assistance Communications



*“Here’s the hard truth: In West Africa, Ebola is now an epidemic of the likes that we have not seen before. It’s spiraling out of control. It is getting worse. It’s spreading faster and exponentially. . . . So today, I’m announcing a major increase in our response. At the request of the Liberian government, we’re going to establish a military command center in Liberia to support civilian efforts across the region -- similar to our response after the Haiti earthquake. . . . Our forces are going to bring their expertise in command and control, in logistics, in engineering. And our Department of Defense is better at that, our Armed Services are better at that than any organization on Earth.”*

- President Barak H. Obama  
September 16, 2014



By LTC Matthew J. Foulk  
MAJ Joseph L. Heyman  
CW2 Reba Wallner

All commanders facing combat appreciate the long-established reality that “War is the realm of uncertainty” (Carl von Clausewitz, *Vom Kriege*, Book 1). War doesn’t always go as expected – hence, the military’s emphasis on planning and adaptability.

The same can also certainly be said of our non-combat missions, such as humanitarian aid and disaster relief, which by their very nature often introduce conditions, not accounted for by standard contingency planning or ingrained combat instincts.

In a military heavily reliant on information technology for all aspects of mission command and execution, such uncertainty is further complicated by the ever-increasing pace of technological

change and rapidly evolving cyber threats.

Providing robust and reliable communications in these situations depends on the flexibility, creativity, and resilience of Signal Soldiers, as illustrated recently in the establishment of effective communication architecture for Operation United Assistance.

The challenges and successes of this mission provide valuable lessons as the Department of Defense moves toward increased interoperability and the Joint Information Environment.

In September 2014, the G6 staff of 101st Airborne Division (Air Assault) was preparing to embark on a series of training exercises designed to stress our systems and prepare us to enter a theater of war. Having faced a 70% staff turnover during the summer permanent change of station rotation, this exercise would have allowed the new

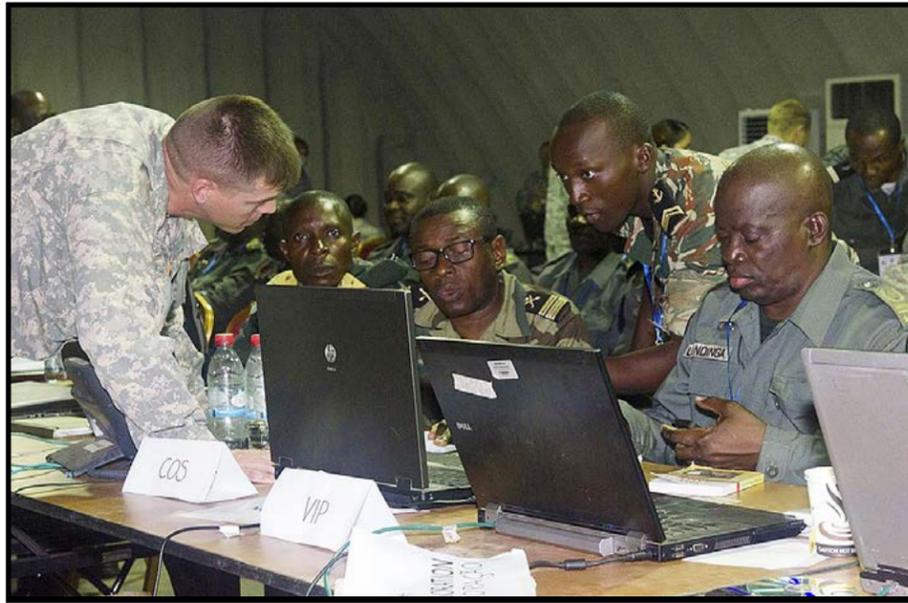
team to train together, assess strengths and weaknesses, and build team cohesiveness. Instead, we received an order to deploy to Liberia, as the 101st assumed the role as the Joint Forces Command for OUA. We hastily organized our deployment and hurried our Soldiers out the door and onto the continent to begin assessing the situation.

## Shifting Gears for Operation United Assistance

Under the direction of United States Africa Command, the mission of the JFC was to support the U. S. Agency for International Development in its efforts “to contain and reduce the threat posed by [the Ebola Virus Disease], save lives, alleviate human suffering, and promote internal and regional stability.”

The World Health Organization would establish

(Continued on page 26)



(Photo by SSG Michael Folkerth)

LTC Jonathan Shine, commander, 4th Battalion, 1st Field Artillery Regiment, 3rd Brigade, 1st Armored Division, works with central African military personnel during the preparation phase of Central Accord 2015 in Libreville, Gabon, 14 May. Shine and his counterparts developed a plan of action for events taking place during the exercise. CA 15 exercises mission command proficiency for UN peacekeeping operations, develops multinational logistical and communications capabilities, and improves regional ability to command, control and support forward deployed forces. Approximately 400 military personnel from member nations are scheduled to participate in the exercise. The exercise consists of one week of classroom-based academics and one week of a command post exercise.

(Continued from page 25)

the requirements and coordinate the provision of medical services and training to medical teams, healthcare workers, and non-governmental organizations. The military's role was to support USAID with mission command, engineering, logistics, equipment, and training. The JFC also had to be prepared "to respond to [Department of State] requests for security or evacuation assistance in the event of a breakdown in civil authority to protect U.S. personnel and facilities."

This was a mission unlike those for which we normally plan. Instead of fighting enemy soldiers, insurgents, or terrorists, our enemy was the deadly Ebola virus. Instead of taking charge

and commanding the effort, we played a supporting role. Like in combat, we were cooperating with USAID and other Federal Agencies, foreign governments, and non-governmental organizations.

Perhaps the biggest change for the signal element of our mission was the need to communicate outside our own secure networks. In our training and combat roles, we tightly restrict information access and communication to our internal team members using our own classified systems (e.g. Secret Internet Protocol Router Network). In OUA, however, we would need to communicate with a wide variety of partners, none of whom had access to our systems. Since an Army division is not fielded with servers for

Non-Classified Internet Protocol Router Network, our standard communication packages would not allow us to communicate with our partners.

In plain language: you can't send an email from a SIPR account to a non-secure account, or the other way around.

Similarly, you can't make a telephone or video call from a classified or secure line to a non-secure line. They are simply not connected. By design, this isolation is intended to ensure sensitive or classified information does not "leak" into the public or enemy hands – a protective measure essential in our traditional missions, but counter-intuitive when your intended audience is the public or non-secure partners.

We quickly realized that to be successful in OUA, we must develop a communication capability outside the standard deployable secure network. Providing basic access to the Internet and Department of Defense Information Network could be achieved fairly simply, but sending email is only a narrow aspect of the network services needed to command and operate in combat or non-combat missions. Our operations depend on services such as enterprise email integration, the Defense Switch Network voice system, portal tools, user authentication and login, and storage area network, to name a few.

### Extending the AFRICOM Network to the Tactical Edge

Requiring these services, the choice to utilize the AFRICOM network domain proved the logical and best-serving option. Fully implemented, this domain would provide the most direct

connection with the command and control element of the JFC's higher headquarters. Users would have access to their existing enterprise email accounts, as well as the full suite of network and system tools. Additionally, enterprise-level network management and defense would be performed by the Regional Cyber Center-Europe, relieving the JFC's J6 section from this task and allowing them to focus on tactical management. Most importantly, we would be able to communicate with our partners to fulfill our mission.

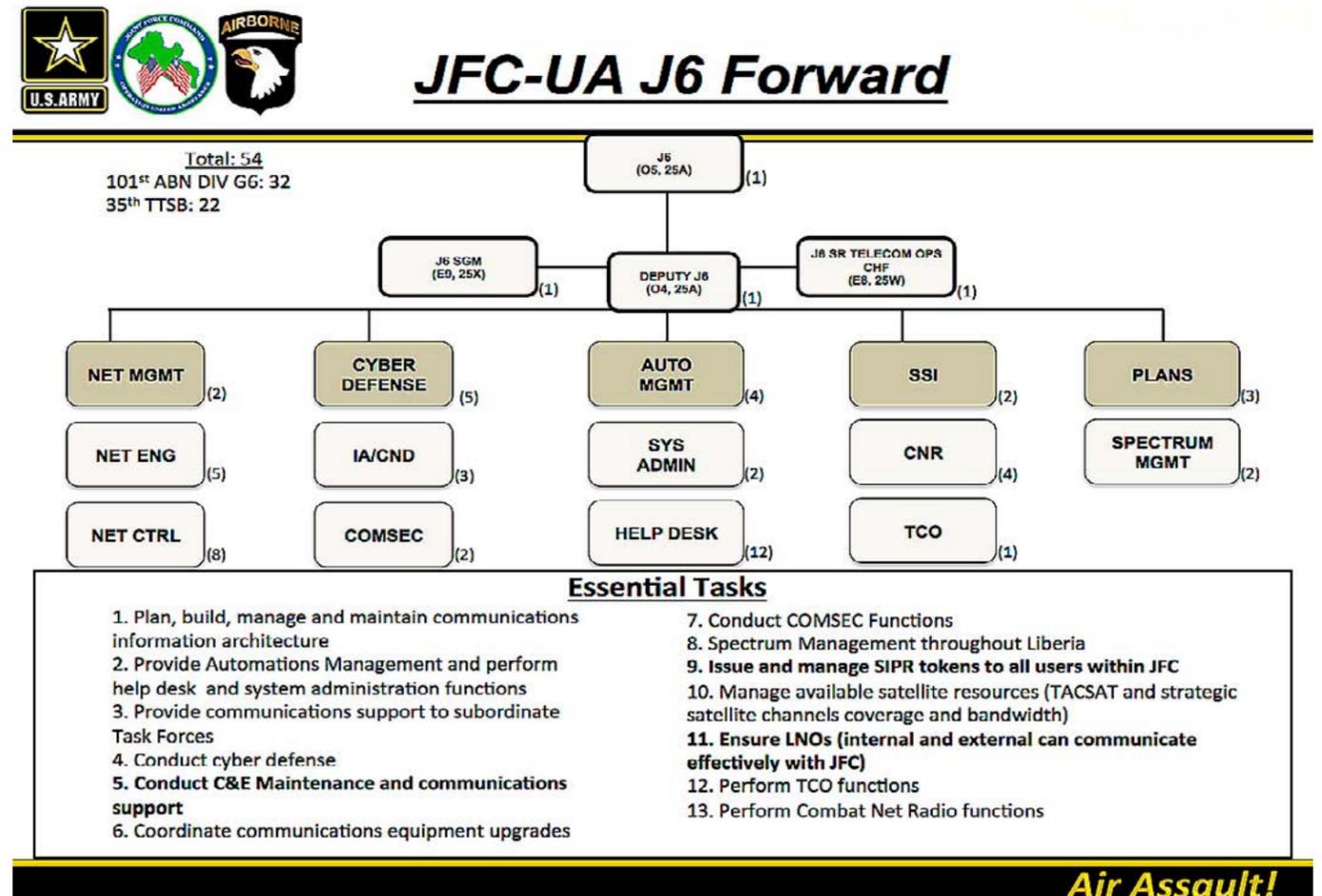
Although the AFRICOM network would provide the best service, extending it to the tactical environment posed several challenges in terms of equipment, network architecture, and data transmission path. From satellite, radio, and fiber transmission sources, to individual computers and telephones – and everything in between – this network would have to support nearly 3,000 personnel in six locations spread throughout the dense jungle of West Africa.

Resources from multiple units would join forces to bring it about. AFRICOM would provide policy, governance, command and control, and critical network services, plus the key NIPR and SIPR server stacks to tunnel into the AFRICOM network. The 5th Signal Command would operate the backbone architecture to reach those services and perform the enterprise network defense mission through the Regional Cyber Center-Europe. The Joint Communications Support Element would provide initial entry communication assets, with follow-on equipment provided by the 101st Airborne Division and 35th Theater Tactical Signal Brigade, who also augmented the JFC J6 staff section.

### Initial Setup

Already on the ground in Liberia, U. S. Army Africa was tasked with the initial planning and command and control mission. Based in Monrovia,

(Continued on page 28)



**Air Assault!**  
(Graphic by MAJ Jason Foreman)

Task organization of the 101st ABN DIV (AASLT) G6 section and 35th TTSB augmentation into the JFC-UA J6 section. The figure also shows the section's essential tasks during OUA.

(Continued from page 27)

this headquarters was supported by two Rapid Response Kits, providing core communications capability for a limited number of users. The Special Purpose Marine Air Ground Task Force at Roberts International Airport and Intermediate Staging Base Senegal were also operating on Rapid Response Kits provided by JCSE or other Services. None of these kits, in the early entry architecture, could provide access to the AFRICOM domain. Collaboration and communication was still available through email and non-AFRICOM portals (such as Intelink), but the common computer domain solution would rely on the provisioning of AFRICOM server stacks and Warfighter Information Network-Tactical equipment.

Such were the conditions when the 101st stood up the Joint Forces Command, facing an impending influx of personnel.

The existing communications resources would be insufficient in terms of both capacity and

functionality, and the establishment of a sufficient network would require the ingenuity and flexibility of a strong J6 section.

In addition to the 32 G6 personnel from the 101st, the 35th TTSB augmented the J6 staff by 22 personnel. Our teammates from the 35th helped us with network management, plans, automation management, and communications and electronics maintenance. This helped to bolster our capability to provide management and oversight to a diverse and geographically dispersed operation in a very short timeframe.

The J6 element that would provide the most flexibility was built into the Signal Systems Integration section. The SSI team handled all of those missions that do not fit nicely into a communications core function (telephone control, SIPR/NIPR Access Point configuration, and Blue Force Tracker configuration, to name a few). Ironically, this tremendously valuable section has been removed from the fiscal year 2015 Division Modification Table of Organization and Equipment.

In addition to the J6 management function, a critical capability enabling initial operations was the provisioning of cell phones and mobile devices. Considering the need to communicate with the outside world, the secure voice system was of no use, and relying on the DSN network would have excessively burdened the bandwidth capacity of our tactical assemblages.

Thanks to the leapfrog effect in developing countries, robust cellular technology has been established in many areas of the African Continent, including Liberia. At a relatively low cost, we issued over 400 cell phones in the first three weeks of operations, allowing critical voice communications among all stakeholders. The use of other mobile devices (e.g. iPads, Blackberries) connected to the cellular system provided commanders and key staff members with on-the-move communications throughout the entire operation. Giving them the speed and flexibility to react to the ever-changing operational environment.

### Transition to AFRICOM Domain

Personnel and equipment were flowing in to Liberia's lone functioning airport creating a bottleneck that delayed the arrival of critical mission command equipment.

On 15 November, three weeks after the transfer

of authority from USARAF to the 101st, Army Warfighter Information Network-Tactical equipment arrived in theater, and the 50th Expeditionary Signal Battalion began a validation exercise at Roberts International Airport. Within two days, the first WIN-T assemblage, Command Post Node 57135, provided services to the 53rd Movement Control Battalion at Roberts, which allowed Joint Task Force Port Opening to redeploy. Three days later, Joint Network Node 5713 and CPN 57133 opened service to Task Force Rugged and Task Force Eagle Medic at the National Police Training Center. Over the next two weeks, incoming WIN-T assets replaced the remaining JCSE Rapid Response Kits, providing full communication support, solving the capacity and functionality limitations, and enabling the JFC to fully execute its mission.

The establishment of the WIN-T assets within the Joint Operations Area finally delivered the originally engineered AFRICOM domain services throughout the JFC.

However, the relief-in-place with JCSE assets also caused turmoil during what was still the early entry phase of OUA. Since WIN-T assets were drawing services from a different entry point into the Department of Defense information network, phone numbers assigned to the Task Forces changed. In addition, users were forced to swap their originally issued JCSE computers for unit-organic computers with AFRICOM domain images. Neither of these events were show stoppers, however it introduced a lot friction into an already tumultuous situation.

The unique architecture also presented distinct challenges in transport and routing. For the WIN-T assemblages, the AFRICOM domain extension was created by tunneling the Internet Protocol traffic from the entry point at the Regional Hub Node in Landstuhl, Germany, directly to the AFRICOM network.

Initial establishment of these tunnels required intense routing and firewall troubleshooting, but after setup the service availability remained high. At the DJC2 supporting the JFC headquarters, engineers took a different approach since AFRICOM servers and network equipment were already in place there. A tunnel was created from the DJC2 through the JCSE network and the Defense Information systems Agency core before finally terminating at the AFRICOM network. These two tunnels, for the first time, placed a tactical unit on a COCOM's domain.

Overcoming these architecture challenges uncovered opportunities to exploit transmission sources not typically available in a tactical environment. As the JFC headquarters grew to almost 200 users, it quickly began to saturate the DJC2 satellite capacity.

One major improvement was the purchase and installation of a 20 Mb circuit provided by LibTelCo, the local internet service provider. After thorough stability and connectivity testing, the NIPR local server stack and users were disconnected from the satellite architecture and connected to the internet service provider.

The NIPR stacks formed a virtual private network directly to AFRICOM, allowing a secure connection through the

commercial internet connection. The ISP provided twice the bandwidth and half the latency for NIPR usage.

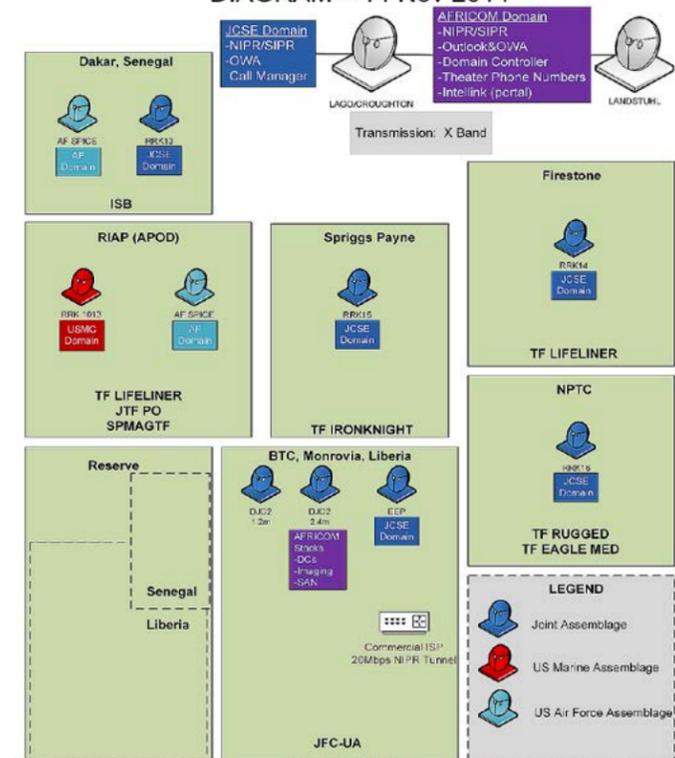
Since the tunnel was transmission-agnostic, J6 Network Operations personnel could move between available transmission sources as those sources came in and out of service. Both SIPR and voice services continued to traverse the satellite, but at a much lower bandwidth utilization rate.

The ISP also allowed a way to provide unclassified network access to users who did not have AFRICOM accounts, such as British and German Liaison Officers, NGOs, and USAID. This allowed us to share the JFC best practices across the JOA.

AFRICOM provided an extensive amount of support throughout each phase of the operation. Often they led the planning efforts and provided initial communications capabilities by leveraging JCSE. They also provided continuous support throughout the actual mission, assisting with troubleshooting and ensuring full data and voice services to each location within the JFC footprint. The domain services allowed for Domain Controllers/Active Directory, CAC-authenticated logons, distributed file services, folder redirection services, a shared drive, and cyber security that would not otherwise have been available. In addition to authentication, authorization, and accountability, the Regional Computer Emergency Response Team and AFRICOM established an umbrella of security, identifying vulnerabilities such as unauthorized devices and cross-

(Continued on page 30)

OPERATION UNITED ASSISTANCE PoP  
DIAGRAM - 14 Nov 2014



(Graphic by MAJ Joseph Heyman)

OUA Communications Nodes prior to the arrival of WIN-T equipment.

domain violations – a tangible benefit of applying the Joint Information Environment in the tactical environment.

### Signal Soldiers' Creativity and Dedication

The very establishment of a robust network under such austere conditions and in so short a timeframe is a testament to the hard work, creativity, and dedication of Army Signal Soldiers. Their mettle was repeatedly tested as they pushed the envelope and stretched beyond their core competencies to develop innovative solutions to complex problems.

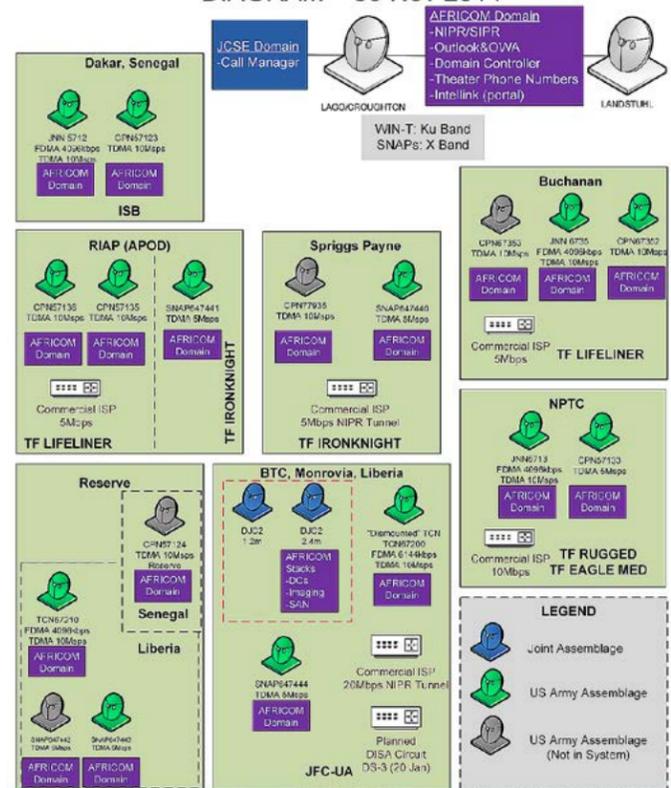
A specific example of this was the use of regular old Army ingenuity to execute specialized and extremely technical work normally performed by contracted Field Service Representatives – a resource on which the Army has become heavily reliant over the past 13 years of deployments. Because of the nature of the Ebola Virus Disease and the heightened risk of exposure, we were not able to bring FSRs. With only one AFRICOM system administrator on ground, the J6 network operations technicians stepped up to fill those roles, quickly becoming proficient at over-the-phone troubleshooting and support for multiple operators. Collaboration and conference calling among various assemblages allowed operators from working terminals to guide non-working terminals through the steps to configure systems and fix problems.

Elsewhere, our J6 team established the first-ever Blue Force Tracking system on the continent of Africa – again without the use of FSRs. In an environment with very limited ground transportation, Task Force Iron Knights provided critical re-supply and transport missions via 14 rotary wing aircraft deployed to support OUA.

Tracking these aircraft in a landscape of 80% dense jungle was imperative, but the BFT capability had to be built from scratch. Receiving this mission on short notice did not allow configurations to be pre-loaded, so all of the programming would have to be done in country with telephonic support from the Communications-Electronics Command in the rear. A satellite was repositioned to provide BFT coverage, and a team of SSI soldiers deployed to the two airfields to install and program the equipment.

In addition to greatly facilitating aviation operations, this capability proved to be a critical lifesaver when on the night of 13 December, a helicopter was forced to make a precautionary

### OPERATION UNITED ASSISTANCE PoP DIAGRAM – 30 Nov 2014



(Graphic by MAJ Joseph Heyman)

### OUA Communications Nodes once all WIN-T equipment was in system and supporting users throughout the JOA.

landing in a remote location not accessible by vehicle or foot.

The Joint Operations Center was able to obtain the 10-digit grid coordinates for the aircraft and immediately dispatch another aircraft to assist. Without the dedication and ingenuity of our signal Soldiers in establishing the BFT architecture, it would have taken much longer to locate them.

### Lessons Learned

Although humanitarian aid and disaster relief missions are not traditional roles for an Infantry Division, they provide invaluable experience to support all aspects of our profession. In the communication realm, our experience highlights the tremendous need to establish the Joint Information Environment and achieve the effectiveness, functionality, and security that it offers. Our collaboration with an array of partners in OUA also provides real-world context to strengthen our drive toward interoperability. As with Haiti in 2010, OUA provides important lessons for future success:

First, commanders – and especially signal

staffs – must be prepared to utilize every available resource in establishing effective communications. The solution to a communications issue may not always come from the Army's inventory. It may come in the form of a \$10 cell phone or a contracted local Internet service provider. The military must learn to operate in conjunction with the existing infrastructure, rather than relying wholly on costly and limited self-contained communications.

Second, we must regain our initial entry capability. In OUA, the DJC2 and small communications packages from JCSE provided that critical initial entry capability. This wasn't the JFC's preferred solution to early entry communications, but was instead driven by the simple fact that JCSE could get to the fight first. The Army's initial entry communications capability gap must be addressed if we are to return to the expeditionary proficiency we once had.

Third, we must invest in deepening and broadening the expertise of the signal Soldier. Our solutions in OUA prove that we are capable of this. As we take the common-sense approach of utilizing existing commercial technology, we must move away from a dependence on contracted knowledge and expertise. Our Soldiers must know how to strengthen our security and functionality, leveraging multiple capabilities within the ever-changing pace of technological advancement.

Finally, we must get back to the basics of human communication. Our signal success in OUA derived not purely from specialized technical acumen and cutting-edge technology, but from the vision of our leadership and the willingness of personnel from multiple organizations to work together as a team. Under such leadership, the combined efforts of AFRICOM, USARAF, and the

101st G6, along with JCSE, 5th Signal Command, and 35th Theater Tactical Signal Brigade, led to the successful installation of a reliable communications infrastructure, enabling the life-saving efforts of the operation.

*LTC Matthew Foulk is currently the G6 for the 101st Airborne Division (Air Assault) at Fort Campbell, Ky. He deployed as the J6 for Joint Forces Command-Operation United Assistance, combating the Ebola virus in Monrovia, Liberia. He also deployed as the S6 for the 2nd Brigade Combat Team, 82nd Airborne Division during Operation Unified Response, the U.S. response to the 2010 earthquake in Haiti.*

*MAJ Joseph L. Heyman is currently the Network Engineer for the 101st Airborne Division (Air Assault) at Fort Campbell, Ky. He deployed as the J6 Network Engineer for Joint Forces Command-Operation Unified Assistance. He was previously an assistant professor in the Electrical Engineering and Computer Science Department at the United States Military Academy. MAJ Heyman received a Master of Science in Electrical and Computer Engineering from Carnegie Mellon University in 2011.*

*CW2 Reba Wallner is currently the senior Network Technician for the 101st Airborne Division (Air Assault) at Fort Campbell, Ky. She deployed as the J6 Network Technician for Joint Forces Command-Operation United Assistance. She also deployed as a CJ6 Network Technician for 101st Airborne Division during Operation Enduring Freedom in Afghanistan and as the Brigade Network Technician for the 3rd Brigade Combat Team, 4th Infantry Division during Operation Iraqi Freedom/Operation New Dawn in Iraq.*

### ACRONYM QuickScan

**AFRICOM** – U. S. Africa Command  
**BFT** – Blue Force Tracking  
**CAC** – Common Access Card  
**COCOM** – Combatant Command  
**CPN** – Command Post Node  
**DJC2** – Deployable Joint Command and Control  
**DSN** – Defense Switched Network  
**FSR** – Field Service Representative  
**ISB** – Intermediate Staging Base  
**ISP** – Internet Service Provider

**JCSE** – Joint Communications Support Element  
**JFC** – Joint Forces Command  
**JOA** – Joint Operation Area  
**Libtelco** – Liberia Telecommunications Corporation  
**NIPRNET** – Nonsecure Internet Protocol Router Network  
**NGO** – Non-Governmental Organization  
**OUA** – Operation United Assistance

**RRK** – Rapid Response Kit  
**SIPRNET** – Secure Internet Protocol Router Network  
**SPMAGTF** – Special Purpose Marine Air Ground Task Force  
**SSI** – Signal Systems Integration  
**TTSB** – Theater Tactical Signal Brigade  
**USAID** – U. S. Agency for International Development  
**USARAF** – U. S. Army Africa  
**WIN-T** – Warfighter Information Network-Tactical

# Partnerships in Europe Mixed Signals

By MAJ Natalie Vanatta  
CPT Robert Singley and  
CPT James Torrence

*Even decades after the collapse of the Soviet Union, the North Atlantic Treaty Organization continues to be the world's most important military alliance (Economist, 2015). The strength of this alliance comes from the 28 countries that make up NATO and their dedication to cooperation and partnership. LTG Ben Hodges, U.S. Army Europe commander, said the United States "needs the capacity that other countries can bring. In a world where the U.S. can no longer afford (economically, militarily, and politically) to be the lead on every action, we must develop and sustain strong partnerships in order to be successful."*



**"OPPORTUNITIES LIKE THIS... THIS IS WHERE INITIATIVE, CREATIVE THINKING, CREATIVE TRAINING OPPORTUNITIES ARE REALLY GOING TO BE WHAT ALLOWS THIS TO WORK."**

**-CPT. JACOB ROECKER  
COMMANDER, C/44 ESB**

44th Signal Battalion and the 383d Communication and Information Systems Battalion conducted a joint small arms range in Grafenwoehr.

This article explores how the European Signal community is accepting the challenge to create lasting and meaningful partnerships with our allies.

### **Why develop partnerships?**

In the fiscally constrained yet dynamic environment of Europe, we routinely operate at 2010 funding levels yet have more combined operations occurring than any other theater. Our Soldiers embody the concept of ready and resilient. They routinely work with Soldiers from other nations in order to accomplish the mission and maintain peace.

The diversity this represents in training opportunities, operational concept sharing, and cultural experience is a strength gained from partnerships. President Obama, during the 2014 NATO Summit, remarked "First and foremost, we have reaffirmed the central mission of the Alliance. Article 5 enshrines our solemn duty to each other - 'an armed attack against one...shall be considered an attack against them all.'" (whitehouse.gov, 2014) Developing a relationship with our partners is important in order to further strengthen NATO as well as to be successful in future armed conflict.

Partnerships need to be created at the tactical, operational, and strategic level. These partnerships ultimately create valuable training experiences for our Soldiers while building power projection platforms to deter theater threats.

Once such partnership is between Bravo Company, 44th Expeditionary Signal Battalion and the 250 Gurkha Signal Squadron. In order to maintain interoperability between signal assemblages, the two units participate in an annual exercise called "Stoney Run." Unit planners base the training scenario around real world events affecting the European theater. The scenario adds realism to exercise which is centered on passing data through respective systems using IP-based routing, telephony, and line-of-sight.

After the exercise the partners engage in friendly sporting competitions while sharing food from their respective countries. The technical portion of the exercise lays the ground work for the future, while it is the human side of the engagement which strengthens the alliance and helps to foster the partnership.

(Continued on page 34)

(Continued from page 33)

### Signal Partnerships

The requirement to develop successful partnerships with NATO and partner-nations does not rest solely on the shoulders of tactical maneuver units. Signal units play an important role in establishing and maintaining partnerships by enabling mission command. In Afghanistan, Commanders saw a need to share information and communicate with multinational units across the battlefield. The International Security Assistance Force's evolving mission made it apparent to leaders that timely information sharing and the creation of a shared awareness would increase overall operational efficiency. In 2009, the commander of ISAF, GEN David McKiernan, approved the development of the Afghan Mission Network. In 2010, Initial Operational Capability was achieved and in 2011 there were 48 NATO and partner-nations operating on AMN. AMN is not the end-state for an allied mission network, but it is a real-world example that clearly highlights that when a need exists, the technical creation of a coalition network is relatively simple. Our difficulty comes from a need to shift from "limited distribution of information" to an "information sharing" culture.

In an effort to reach LTG Hodges' vision of an interoperable European land force, 2nd Signal Brigade must turn the combination of unique capabilities in distinctive battalion areas of responsibility with disparate partners into a viable, secure and stable communications network. Adhering to the philosophy of mission command, each battalion determines what partnership in their AOR means and actively pursues it.

The end state of this objective is to strengthen current social and business relationships while building technical relationships that extend our network capabilities. One output from the process was the creation of the Austere Challenge Mission Environment. It began as a collaborative mission partnership environment to support allied partner exercises developed by individuals within the BDE, 5th Signal Command, and USAREUR G6.

This solution, recently renamed the Army Coalition Mission Environment, will be fully integrated with NATO core services and systems during Steadfast Cobalt 15 in Poland this summer. The 102nd Signal Battalion began their partnership with the 282nd Bundeswehr Command Support Battalion with a host of training and socialization events. In March, they successfully communicated via High Frequency radio between command

posts. The two battalions are now planning a communications exercise that will demonstrate the possibilities for communications interoperability (voice and data) between coalition partners utilizing different media. Further south, the 509th Signal Battalion is participating in Bold Quest, the U.S. Army Training and Doctrine Command's Network Integration Evaluation 16.1 in which an Italian Airborne unit conducts a Joint Forcible Entry Operation as part of a multinational division operation. This event will test the Italian's ability to mission command subordinate units via 509th's strategic connectivity.

### Challenges

The last decade of war has thrust the U.S. into a position where partnerships with NATO and allied nations are essential to maintain peace, stability, and cohesion in an ever-changing operational environment.

The need for lasting partnerships has institutional, technical, and cultural challenges for U.S. forces. Some of these challenges can be met at the unit level while others require senior leader attention if we hope to shape our force into valuing partnerships.

### Institutional Challenges

The need for partnership has outpaced both our military education system and the Mission Essential Tasks by which a unit is assessed. In order for partnership to be successful in the Army it should become a part of curriculum in TRADOC courses and become a MET assigned to units asked to partner with a foreign nation.

The Army concept of "train as we fight" has been around for decades. It is an underlying principle that creates a premier fighting force. Partnerships are how we fight today. TRADOC has spent extensive resources providing simulations and communications platforms to schoolhouses in order to train Soldiers. In fact, the latest version of FM 6-02 (Signal Support to Operations) covers the importance of "providing Soldiers the capability to train on the same warfighting applications terminals used during deployment."

Even with the doctrinal requirement of creating an environment similar to a deployed one, schoolhouse training does not occur on combined communications platforms essential to allied operations. Providing an awareness of the variety of networks, the countries that can access them, and the constraints on information sharing would be beneficial to Soldiers.

NATO Mission Secret Network, Battlefield Information Collection and Exploitation, and Coalition Network are frequently found in European allied operations and Signaleers are expected to be familiar with them. Ask a Signaleer about why we can share SECRET information with Australia. Chances are they do not know the answer.

However, it came from the partnership and trust developed between the five countries (now known as Five Eyes) as they worked in Bletchley Park to break codes during WWII. Understanding how we are authorized to share information between countries is integral in being able to develop and defend shared communications networks (a primary task of a Signal Soldier).

According to FM 7-15, there are no Army METs that deal with allied nation partnership. The Universal Navy Task List which includes the Navy, Marines, and Coast Guard does not have any tasks dealing with coalition partnership. In fact, Joint doctrine only has two tasks in the Universal Joint Task List with the word partnership.

While the USAREUR Commander's intent espouses partnership as being paramount to success, there are still no means for the evaluation of individual units if the value of partnership is not quantified as a MET. Although partnership is not a new concept it has never been captured or codified in our handbook of what we do. Partnership should be a MET in the European Theater where combined operations continue to increase (both in number and frequency) and communications interoperability is essential.

### Technical Challenges

Along with the challenge of properly educating our military on partnerships, there are also technical challenges in maintaining partnerships. From a signal perspective, the challenge is creating communications interoperability.

Communications interoperability is the integration of tactical and strategic communications platforms resulting in: secure line of sight/beyond line of sight communication capabilities between units, position location information of combined forces which feeds into a common operational picture, and a shared network that facilitates mission command amongst combined forces. According to COL Jimmy Hall, commander 5th Signal Command, "interoperability is critical to mission success because the very fabric and strength of a unit relies on our ability to be interoperable whether it's in the Combat

Arms arena, through direct support or in an Enabler organization."

Looking at the development of communications capabilities with U.S. forces over the last two decades, we still struggle to ensure an Army Soldier can call for fire from an Air Force or Navy unit without a liaison on the ground. We struggle to convince acquisition entities and senior service leadership to champion communications equipment that is interoperable. Now we need to convince foreign countries that we should all purchase and use technology that would enable interoperability.

This enormous challenge cannot be tackled overnight. Short term efforts should focus on re-purposing existing technology to achieve an initial level of communications interoperability. There are three primary goals within Europe. First is to talk secure FM between company headquarters of allied forces. Second is to feed information on units (position, disposition) into a higher headquarters COP. Third is to provide a communications backbone that allies can access and reach back to their home station. While this does not sound overly difficult, U.S. units engaged in Operation Atlantic Resolve can only organically communicate with tactical Polish units via plaintext FM and not at all with many others. This should be very troubling. Without shared communications – partnerships fail.

At the strategic level, the 39th Signal Battalion's Communications team supporting GEN Breedlove, Supreme Allied Commander Europe, is leading the effort to provide him with updated, secure data capabilities; a secure cross-domain solution for complete two-way classified message traffic and attachment functionality between SIPR, BICES, NMSN, and others. While other DODIN domain solutions have been used around the globe – this is a holistic system that will enable SACEUR to communicate with his staff.

Finally, long term solutions (7-10 years) are also needed to facilitate communications interoperability amongst our allies. Technical solutions are easy; the challenge is getting a group of people moving toward the same objective. Personnel from the communities of intelligence, communications, logistics, operations, acquisitions, NATO, and host-nation representatives must conquer the challenges presented by a host of issues that include a varied communications capabilities, security measures, acquisition policies, and country regulations in order to develop a

(Continued on page 36)

(Continued from page 35)

functional and interoperable solution.

### Cultural Challenges

If we are able to tackle the educational shift in our thinking towards valuing partnerships and develop fieldable, technical solutions to handle the challenges of communications interoperability that will still leave us with many cultural challenges. These cultural challenges, both internal as well as external, play an equally important role when developing lasting partnerships.

One internal cultural challenge is the existing stigma that assignments with foreign nations are easy and “away from the flagpole.” More value is placed on a “combat” tour in Kuwait than a year embedded in a foreign military speaking their language,

learning their doctrine, being an ambassador for the U.S. military, and learning how we can better work together when deployed to face a common foe. There needs to be a paradigm shift amongst leaders in the military to embrace the opportunities to interact with our foreign allies. Combined assignments result in a force that understands how and why foreign militaries conduct operations; they result in enduring relationships and enhance leader education and development.

Pick a typical day in a NATO Task Force. You might see a company-grade foreign officer (that is not a native English speaker) briefing a 4-star general on battle plans that will affect combat operations. This clearly shows how other countries value their partnerships (to spend the time training leaders on

other cultures and languages). Of course, the easy answer is that the U.S. has Foreign Area Officers to handle these situations. That is a fallacy we need to overcome in the U.S. military. Every Soldier is an Ambassador, and partnership is not a specialized job for only a few. This must be one of the many tasks required of the American Soldier, NCO, and Officer.

There are also external cultural challenges when creating partnerships. The first is language related. Different countries provide different levels of resources/ requirements for their populations to learn English. Therefore, the ease of a company commander speaking to his Hungarian counterpart vice his British counterpart might be different. Another cultural difference is planning cycles. The U.S. Army locks in unit training six weeks in advance. Perhaps significant large-scale training events are scheduled six months in advance. However, typically Italian units lock in their unit training at least 12 months in advance and normally closer to 24. Additionally, challenges can arise from partnering with countries with different societal values, economic structures, and requirements for military service. Therefore, the evolution of their militaries can be significantly different than our own. Finally, the greatest challenge is in cultivating and maintaining trust within the partnership despite our differences.

With over 51 countries in USAREUR’s area of responsibility, multiple multinational exercises, and the possibility of real world missions, the European theater is a constant leadership lab for those fortunate enough to support these efforts. However, to truly enable the alliance, one must go beyond exercise participation.

Leaders should seek to build successful, active partnerships with NATO allies and partner-nations. According to author Jack Schafer’s book, *The Like Switch*, friendships are influenced by the principles of proximity, frequency, duration, and intensity. In order to build successful relationships, units should find organizations within the theater that they can plan training events with. These events can span from social to tactical.

Furthermore, these partnerships should be constantly developed over time through multiple engagements that will add positive value to both units. The 52nd Signal Battalion embodies this concept as they partner with a local German Reserve Association. With a focus on cultural exchange, they have jointly participated in field training, land navigation, warrior task-based competitions, Christmas parties, and other events.

Those not within the theater should look forward for how they may prepare themselves for the future of unified land operations worldwide. Cultural, linguistic, and doctrinal training centered on our partners will act as a force multiplier allowing us to better understand our coalition team members and build lasting relationships.

### Conclusion

When it comes to understanding the importance of our European allies, U.S. troops stationed overseas in the European theater have a distinct advantage over their state-side peers. Not only are Soldiers immersed in European culture during their tour, they also have many opportunities to participate in multinational training events. Although the cultures may differ, many of our partner nations have similar units, task organization, or mission statements which

help to bridge the cultural gap. These partnerships are important in preparing NATO and partner-nation armies for stability, defensive and offensive operations all while fostering interoperability and trust. We must train our Soldiers and leaders to be flexible in their thinking, understand that sometimes they must lead and other times they must follow, and we must recognize that everyone has a contribution to make when addressing multinational problems.

*CPT James Torrence is a Signal Corps Officer currently serving as the Company Commander of the 128th Signal Company, 39th Signal Battalion. He holds a B.S. from West Point, an M.S. from California University of Pennsylvania, and an M.S. from American Military University. He has deployed twice as a Battalion Signal Officer in a Brigade Combat Team and spent the last two years serving in a Joint and Combined strategic communications environment.*

*CPT Robert Singley is a Signal Corps Officer currently serving as the Company Commander of Bravo Company, 44th Expeditionary Signal Battalion in USAG Bavaria. He holds a B.S. from West Point and an M.S. from the University of Maryland University College. He has deployed twice to Iraq as a platoon leader and Battalion Signal Officer and once to Afghanistan as an aide to the ISAF CJ6.*

*MAJ Natalie Vanatta was commissioned in the Army Signal Corps through the ROTC program. She is one of the first Army Cyber officers and is currently serving as the 509th Signal Battalion Executive Officer in Italy. She has her PhD from Naval Postgraduate School and multiple M.S. degrees. She has worked from tactical to operational levels in the signal arena around the world while also teaching/researching in the cyber field.*



SSG Callahan, 44th Signal Battalion platoon sergeant, discusses M16 capabilities to his German counterpart.

### ACRONYM QuickScan

AMN - Afghan Mission Network  
BICES - Battlefield Information Collection and Exploitation  
ISAF - International Security Assistance Force  
MET - Mission Essential Task  
NATO - North Atlantic Treaty

Organization  
NMSN - NATO Mission Secret Network  
SACEUR - Supreme Allied Commander Europe  
TRADOC - U. S. Army

Training and Doctrine Command  
U.S. - United States  
USAREUR - U. S. Army Europe



Signal Regiment member, GEN Dennis Via, U.S. Army Materiel Command commanding general, participated in the festivities at the 2015 Signal Corps Regimental Ball.

# Enabling Success



LTG Robert S. Ferrell addresses participants gathered on 27 March in Springfield, Va., for the 2015 Signal Corps Regimental Ball.



The evening was filled with sights and sounds of celebration as the gathering of Signal Regiment members and their guests ate, danced, and fellowshipped at the 2015 Signal Corps Regimental Ball.



# for Today and Tomorrow

*“Our 2015 Signal Corps Regimental Ball was a terrific opportunity to commemorate the dedication, courage and rich traditions of the U.S. Army Signal Corps. More than 500 guests attended and we were especially honored to have General Dennis L. Via, Commanding General, U.S. Army Materiel Command as our guest of honor and speaker. The recognition of five new 'Distinguished Members of the Regiment' proved to be a highlight of the evening.”*

*LTG Robert Ferrell  
U.S. Army Chief Information Officer/G6*



# Chief of Signal Awards Program

The Chief of Signal Regimental Awards program is designed to foster esprit de corps and contribute to the Signal Regiment's cohesiveness. This is done, in part, through recognizing the exceptional performance of individuals who merit special commendation from the Chief of Signal.

Awards may be approved by the Chief of Signal based on personal observations or upon an individual's written recommendation. Eligible recipients include personnel, both military and civilian, worldwide.

There are six types of awards/recognition:

Regimental Impact awards are unique mementos presented by the Chief of Signal as "on-the-spot" recognition for outstanding performance or achievement.

The Certificate of Achievement (Fort Gordon Form 6723-1) is used to recognize outstanding achievements relative to the Signal Regiment's mission. The certificate recognizes achievements of a lesser degree than required for the Chief of Signal Plaque or Signal Regiment Fellowship Award.

The Chief of Signal Plaque is awarded to deserving individuals based on recommendations from commanders and supervisors citing outstanding achievement or recognition for special projects relevant to the Signal Regiment's mission. The Chief of Signal Plaque is not to be used as an ETS, PCS, retirement or any other official Army award.

The Fellowship Award is designed to recognize people not

affiliated with the Regiment. The requirements are the same as the Chief of Signal Plaque only the award isn't normally presented to Signal personnel.

The Honorary Member of the Regiment program is designed to recognize soldiers and other individuals who have made a contribution or provided a service to the Regiment, but who are not members of the Regiment. Appropriate recognition is made of active and retired military, Defense Department civilians and other people deemed worthy by the Chief of Signal.

There are no duties associated with this appointment; however, Honorary Members are encouraged to participate in Regimental functions.

Individuals who have been recognized as Signal Regiment Honorary Members include foreign allied exchange/liason officers and noncommissioned officers who have been assigned for duty at the Signal Center, non-Signal Regiment soldiers, and service members of our sister armed forces.

Distinguished Members of the Regiment are prestigious or notable military or civilian persons who are recognized for their accomplishments. They must be current or former members of the Signal Corps Regiment. Nominees may be active, U.S. Army Reserve, Army National Guard or Signal Regiment Department of the Army civilians (active or retired status).

The designation as a Distinguished Member of the Regiment is largely ceremonial and serves to perpetuate the history and traditions of the

Regiment, thereby enhancing unit morale and esprit.

Since Regimental activation, the Signal Regiment has had a program for recognizing people who have made a special contribution or who have distinguished themselves in service to the Regiment. Under the provisions of Army Regulation 600-82 (The U.S. Army Regimental System), all U.S. Army Regiments are authorized to select appointees to the position of Distinguished Member of the Regiment.

There are no limits on the number of Distinguished Members, and their tenure is permanent. The positions are designed to promote and enhance the history and traditions of the Regiment and foster cohesion among members of the Regiment.

The Honorary Colonel, Honorary Warrant Officer and Honorary Sergeant Major of the Regiment are distinguished, retired Army Signal Regiment special appointees who simultaneously become Distinguished Members of the Regiment when appointed to their honorary positions. These appointees serve a three-year tour and participate in command and award ceremonies, speaking engagements at dinings-in and other similar functions which help bridge the gap between the past and the present. When their honorary appointment term ends, they remain lifetime Distinguished Members.

## Criteria and nomination submission procedures for Distinguished Members of the Regiment

Persons who are



Newly inducted Distinguished Members of the Regiment were recognized at the 2015 Regimental Signal Ball (left to right), GEN Dennis Via, Woodrow Norris and SSG Jonathan Norris accepting on behalf of their great-great grandfather, MG (Ret) Joseph Mauborgne, CW5 (Ret) Leslie Cornwall, BG (Ret) Velma Richardson, CSM (Ret) Vernon Praymous, COL (Ret) Joseph 'Jake' Simmons, and LTG Robert Ferrell

recommending an individual for the Distinguished Member appointment, will prepare a justification consisting of a double spaced document of no more than two pages in length. This justification should cover the entire period of service to the Regiment. If the candidate is then selected, a citation will be prepared by the Office Chief of Signal based on this justification. Reviewing existing citations will provide the nominator with the type of subject matter and level of achievement that is required. This justification, using a signed memorandum should be mailed to:

**Office Chief of Signal  
Attn: ATZH-PO  
506 Chamberlain Ave.  
Fort Gordon, GA 30905-5735**

or e-mailed to:

[SIGCOEOCOS@conus.army.mil](mailto:SIGCOEOCOS@conus.army.mil)

This memorandum must contain contact information for both the nominee and the nominator to include physical address, e-mail address, and

telephone numbers. These are used for the purposes of acquiring additional information or notification.

These nominations will be reviewed by a Regimental board as convened by the Chief of Signal.

## Eligibility

Any military personnel who served as a member of the Signal Corps; any functional area 24 or 53 officer who has officially affiliated with the Signal Regiment; any civilian employee who is affiliated with the Signal Regiment. For civilians, this is defined as either any Department of the Army civilian employee who has been employed within the CP34 career field or a civilian from any civilian career field who has worked for a Signal Organization for over ten years. Meeting either of these qualifications results in automatic affiliation with the Signal Regiment.

## Criteria

Service rendered to the Signal Regiment is of such significance

with Regimental-wide impact to clearly place this individual head and shoulders above his or her peers. Although there are no specific time requirements for this award, a nominee is to have long term and continuous service to the Regiment. Each nominee must have spent virtually an entire career in service to the Regiment. It is not necessary for the individual to have served within the Signal Regiment as a military member if subsequent service as a civilian is considered to be long term. There are no grade requirements for this award. In meeting the time element of the criteria, however, all but our most senior members will normally be excluded. For military members, that may also mean that the nominee continued to serve the Regiment in some capacity as a civilian. Regardless of time served or rank obtained, the board shall be empowered to nominate to the Chief of Signal any individual whose accomplishments are of such magnitude that he or she must be considered for appointment as a Distinguished Member.

## Signal Regiment Certificate of Achievement Criteria and nomination submission procedures

Commanders desiring to recommend an individual for the Signal Regiment Certificate of Achievement, Chief of Signal Plaque, or Regimental Fellowship award will prepare a Recommendation for Award (DA Form 638) with a proposed citation subject to the following limitations:

-Certificate of Achievement: no more than nine double-spaced lines

-Chief of Signal Plaque: no more than 15 words, including individual's name

# New Distinguished Members of the Regiment

## BG (Retired) Velma L. Richardson

BG (Ret) Velma L. Richardson has served the U. S. Army and the Signal Regiment with distinction during her 31 years of service, including two tours of duty outside the Continental United States.

Born and educated in South Carolina, BG (R) Richardson was commissioned as a second lieutenant and entered active duty in the Women's Army Corps in May 1973 and served continuously in the U. S. Army Signal Corps until her retirement in October of 2003. Her assignments included: Signal officer, 1st Battalion, 55th Air Defense Artillery, Fort Bliss, Texas; platoon leader and company commander, 51st Signal Battalion; assistant professor of Military Science, Virginia State University; commander, 426th Signal Battalion, later reflagged the 51st Signal Battalion at Fort Bragg, N. C.; commander, 1108th Signal Brigade, Fort Ritchie, Md; deputy commanding general U.S. Army Signal Center and Fort Gordon, Ga.; and deputy commanding general, Army and Air Force Exchange Service, Dallas, Texas.

BG (R) Richardson is one of only nine African American women to have earned the rank of brigadier general on active duty in the U. S. Army, and was the first in the history of the U.S. Army and the Signal Corps to be promoted to brigadier general. She was honored as NAACP Augusta Branch Woman of the Year 2000. Also, she was selected to be included in the BellSouth 2001 South Carolina African-American History Calendar.



**BG (Retired) Velma L. Richardson**

On 23 March 2001 she was recognized as one of the outstanding graduates of historically black colleges and universities at the 26th National Conference on Blacks in Higher Education in Washington, DC. On 23 June 2001, she was inducted into the South Carolina Black Hall of Fame and was twice honored as a Texas Trailblazer while serving at AAFES. She was also recognized by the White House Initiative on Historically Black Colleges and Universities for outstanding service to the nation's military profession in 2003.

Most recently, BG (R) Richardson serves as the Lockheed Martin IS&GS Small Business

Development Principal responsible for setting and managing the strategic direction of the Gulf Coast-based small business/college and university outreach and development program as well as its execution. In this position, she identifies, establishes, coordinates, and monitors challenges associated with implementing IS&GS innovation clusters at designated colleges and universities. Serving as a university coordinator, she builds relationships with key colleges and universities for integration into the LM Internship Program and facilitates mentoring opportunities for university and small business partners.

Prior to this position, she led the Department of Defense Information Technology efforts in Lockheed Martin's Washington Operations unit where she supported Washington-based DoD chief information officers and other IT leaders in identifying priorities, increasing program visibility, taking new technology directions, and recommending innovative IT solutions as their missions evolved. BG (R) Richardson retired from Lockheed Martin in 2013.

BG (R) Richardson's earned a Bachelor of Science Degree in Mathematics from Livingstone College in Salisbury, N.C. and a Master of Arts degree from Pepperdine University in Human Resources Management. Her professional education includes the U. S. Army Command and General Staff College and the U. S. Army War College. She is also a 2005 recipient of the Doctor of Laws Degree (Honoris Causa) from Livingstone College and the Parren

J. Mitchell Foundation Awardee for Excellence.

In October 2005, BG (R) Richardson was recognized as the National Women of Color in Technology's Distinguished Achiever in Leadership.

Recently, she received the ROCK of the Year award from the National Board of Directors of the ROCKS, a non-profit organization focused on mentorship, scholarship and education for current and retired Army officers, warrant officers, and SROTC/JROTC students.

In March 2012, State of South Carolina officials once again honored her as one of the Women in Philanthropy and Leadership Inspiring Woman.

BG (R) Richardson's awards and decorations include the Distinguished Service Medal, the Legion of Merit with two Oak Leaf Clusters, the Defense Meritorious Service Medal, the Meritorious Service Medal with six Oak Leaf Clusters, the Army Commendation Medal, the Army Achievement Medal, the National Defense Service Medal (third award) and the Department of Defense Identification Badge.

## CW5 (Retired) Leslie E. Cornwall

CW5 (Retired) Leslie E. Cornwall enlisted as a Signaleer in the U.S. Army in 1977. He successfully progressed to the rank of sergeant first class then transitioned to the warrant officer corps in September 1992 and finally retiring as a chief warrant officer 5 on 30 April 2012 with 35 years of service.

During his enlisted career he served as tactical circuit controller in 142nd Signal Battalion, 2nd Armored Division, Fort Hood, Texas from July 1977 to June 1979 where he was a major participant



**CW5 (Retired) Leslie E. Cornwall**

in numerous successful brigade and division field training exercises and NTC rotations.

CW5 (R) Cornwall was then assigned as a senior tactical circuit controller/multichannel team chief in 38th ADA (Hawk Missile) Brigade, Osan AFB, Korea from July 1979 to May 1981. He excelled during numerous EDREs and special exercises in ROK and made the smooth transition of the US Army missile communications sites to the ROK Army and the eventual de-activation of the 38th ADA Brigade in May 1981. CW5 (R) Cornwall was then assigned to 122nd Signal Battalion, 2nd Infantry Division (M) from May 1981 to Sep 1981 as the circuit control section sergeant.

He led his section during numerous successful CFC/USFK/

Division exercises and maintained systems/circuit reliability over 95%. CW5 (R) Cornwall was then assigned as the circuit controller section sergeant in C Company, 304th Signal Battalion, 1st Signal Brigade, Camp Colbern, ROK from Sep 1981 to Mar 1982. He was singled out for outstanding performance for at least three impact awards during very successful field training exercises to include Team Spirit 1982.

CW5 (R) Cornwall then changed duty stations back to CONUS to 54th Signal Battalion (Corps Radio), 3rd Signal Brigade, Fort Hood, Texas as a multichannel radio section sergeant from April 1982-April 1984. He was very instrumental in the cross training of troposcatter operators (26Q) and multichannel operators (31M) during a time when there were critical MOS shortages. He then PCS to Europe to the 72nd Signal Battalion, 7th Signal Brigade, 5th Signal Command on Nueruet Kaserne, Karlsruhe, Germany as a battalion network controller from April 1984-April 1987. He provided outstanding communications supporting the largest tactical deployable command posts in Europe; USAREUR Main and Rear and received numerous impact awards during his tenure there. He was the brigade's subject matter expert on TRI-TAC switches and multichannel systems installation and troubleshooting and was a member of the team that engineered and installed the first TRI-TAC digital transmission group across Multichannel Satellite Systems in the Army.

He then returned to the ROK 304th Signal Battalion as the battalion senior network controller from May 1987 to May 1988. He was very instrumental in the

(Continued on page 44)

(Continued from page 43)

rewiring and upgrading of the tactical communications provided to the commander CFC/USFK/8A and his staff at command post Tango and deployed and provided outstanding communications support during exercises Team Spirit, Ulchi Focus Lens and Foal Eagle.

His next assignment was at 447th Signal Battalion (Signal Leadership Department), 15th Signal Brigade, Fort Gordon, Ga., as an instructor/writer from May 1988 to Mar 1991. He taught TRI-TAC and MSE to field grade officers, senior NCOs, and warrant officers' basic and advance courses. His talents were recognized by the course senior warrant officer and he was encouraged to submit a warrant officer application.

He was then assigned on post to the 258th Signal Company, Fort Gordon as a platoon sergeant. He was very instrumental in the successful transformation of the 258th Signal Company from a cable construction company to a MSE Area Company.

CW5 (Ret) Cornwall then attended the Warrant Officer Candidate Course from Mar - May 1992. CW5 (Ret) Cornwall graduated as the distinguished honor graduate from Warrant Officer Basic Course in September 1992. He was then assigned as the 3d Signal Brigade, III Corps Network Technician from October 1992 - June 1995 at Fort Hood, Texas. He excelled provided leadership, expertise and training to the officers, NCOs and Soldiers. He was part of a very successful deployment of III Corps Main and Tactical Command Post to the National Training Center at Fort Irwin, Calif. He was also the leader of III Corps representation on the Signal Regiment Network

Advisory Group.

He was then stationed as the 2d Infantry Division G6 Network Technician in the Republic of Korea from June 1995 - June 1996. He introduced packet switching data, tactical email and file sharing to the division and was the lead technician behind the successful fielding of Enhanced Switch Operation Procedures.

CW5 (Ret) Cornwall returned to III Corps, Fort Hood, Texas as the Senior 3rd Signal Brigade and Senior III Corps G-6 Network Technician from June 1996 - June 2001. During this tenure he led the introduction and integration of high speed multiplexing cards into MSE assemblages which the Army later adopted as the Tactical High Speed Data Network program of record.

CW5 (Ret) Cornwall then attended Training with Industry with General Dynamics in Taunton, Mass., from June 2001 - June 2002 where he assisted industry with Army concepts, deployment strategy and requirements. He was then assigned as the chief network engineer of the Directorate of Combat Development at the U.S. Army Signal Center, Fort Gordon from July 2002 to June 2005 working BBN, MSE/TRITAC Program Improvement Plan, and Task Force - Network, Joint Network Node, WIN-T Increments and numerous other projects. He was an integral part of the team that developed Joint Network Transport Capability Systems as a replacement for the aging MSE systems supporting warfighting headquarters.

CW5 (Ret) Cornwall was then assigned as the chief integrator/senior technical advisor to the director TRADOC Integration Office/Capabilities Development and Integration Directorate,

U.S. Army Signal Center & Fort Gordon, from July 2005 to December 2008 working JNN/CPN improvements, WIN-T Increments, Expeditionary Signal Battalion design and resourcing, OIF/OEF lessons-learned (2 TDY trips to Iraq, 5 TDY trips to Kuwait) and CONOPS.

CW5 (Retired) Cornwall last assignment was to the 7th Signal Command (Theater), Fort Gordon from December 2008 to April 2012 as the command senior warrant officer working Network Enterprise Support Team functions, standardization and configuration management across the Operating and Generating Force in the CONUS Theater. He played a major role in the successful deployment of Enterprise Email across the entire CONUS theater. He deployed to Afghanistan on a hand-picked tasking as the Senior Network Integrator responsible for optimizing the transport network for the CJOA-A.

He is a graduate of the Warrant Officer Staff Course, Warrant Officer Advance Course and Warrant Officer Basic Course in addition to numerous technical courses. His awards and decorations include the LOM, MSM (6), ARCOM (6), AAM (8), NATO Medal, JMUA, AGCM (5), NDSM (3), ACMCS, GWOTE, GWOTS, KDSM, NCO DR (3), ASR, and OSR (4).

He is a graduate of Paine College with BA Degree in General Business.

He is an active member of the following professional organizations; Association of U.S. Army, Warrant Officer Association, Signal Corps Regimental Association - Lifetime Member and Armed Forces Communication and Electronics Association - Lifetime Member.

CW5 (Ret) Cornwall has been recognized with the following; AFCEA Leadership Award - Runner up 2007, SCRA Silver Order of Mercury September 2006, SCRA Albert J. Meyer Award June 2005, SCRA Bronze Order of Mercury June 1995, and AFCEA President's Award Dec 2004.

CW5 (Ret) Cornwall is married to the former Incha (Lee) Yi. They have four children; LT Leslie Jr (USNA class of 2004), Janice (University of Houston class of 2006) and twins Shawn and Sharon (Augusta State University/Georgia State University 2014).

### MG (Retired) Joseph O. Mauborgne

MG Joseph Oswald Mauborgne (1881-1971), 12th Chief of Signals, was born in Brooklyn, N. Y. on 26 February 1881. The son of Eugene and Catherine Elizabeth McLaughlin Mauborgne, he followed an unusual path to what would become a distinguished military career. MG Mauborgne was one of the more technically competent and interesting men to serve as the Chief of Signal.

After earning an AB degree from The College of Saint Xavier in New York City in 1901 the young Mauborgne enrolled in New York's Art Student's League. There he studied the fine arts until he accepted a commission as second lieutenant in the regular Army in 1903.

During his early years as a junior officer he was assigned to a series of domestic and foreign infantry duty stations typical of the service at the time. As part of his professional military education Mauborgne attended the Army Signal School at Fort Leavenworth, Kansas, graduating from the course in 1910. This was followed by a tour of duty in Washington

working in the office of Chief Signal Officer BG General George P. Scriven.

While stationed at Fort Riley, Kansas, in 1912, he installed a radio transmitter in an aircraft and had another lieutenant take him aloft to complete the first successful air to ground radio transmission. At this time there was no separate air arm and all aviation resources and responsibilities in the Army were under the control of the Signal Corps. It was an exciting time to have the two most advanced technologies of the time under one roof and it allowed for this type of experimentation to be carried on with a minimum of red tape.

Both young officers, reaching into the heights that day, would soar still higher until they reached the top of their professions. Mauborgne would eventually become the Chief of the Signal Corps. The pilot, H.H. "Hap" Arnold would rise to five star rank and command the Army Air Force.

Two years later, on 11 December 1914, Mauborgne operated a radio while Lieutenant Herbert "Bert" Dargue piloted a Burgess-Wright biplane over Manila. While Dargue, who would eventually enter the Aviation Hall of Fame, piloted lazy circles Mauborgne received signals on a radio he designed that were transmitted from a station, ten miles distant, on the island of Corregidor at the mouth of Manila Bay. Having proven that radio communication from the air to the ground and from the ground to the air was possible it was only a short leap to the next step. Five days later the pair returned to the air and both transmitted and received radio messages, effectively demonstrating the practicality of



MG (Retired) Joseph O. Mauborgne

radiotelegraphy.

While on a trooper bound for the Philippines for the assignment that led to his radiotelegraphy coup, the young officer whiled away the time in another of his many interests, cryptography. Mauborgne found a solution to the British field code named "Playfair," which was originally developed by the British physicist Sir Charles Wheatstone (who was also famous for inventing the electric rheostat known as "Wheatstone's Bridge" and the concertina). Mauborgne's cracking the "Playfair" cipher, and his work with aerial radiotelegraphy, brought him to the attention of the Chief of Signal who permanently attached him to the Signal Corps in 1916. In the small, pre-WW-I Army, Mauborgne was one of only three officers with any expertise in cryptology.

Working with Gilbert Vernam of the American Telephone and Telegraph Company, Mauborgne, now a major, developed the simplest, yet most secure method

(Continued on page 46)

(Continued from page 44)

of encryption known as the "One Time Pad." Simply put this is a pair of identical pads of paper covered with random nonrepeating letters. The sender encodes a message and then destroys the sheet used. The recipient decodes the message and then destroys the sheet. If there are only two pads, each sheet having random letters, and a sheet is used just once then it is the only system that is unconditionally secure because there will be no patterns, and too little message traffic for a cryptologist to analyze.

During WWI, Mauborgne served as Chief of the Signal Corps Engineering and Development Division. He was also sent to France, and during his overseas tour he served as the technical advisor to the U.S. delegation at the Inter-Allied Radio Conference in 1919. Mauborgne received the Distinguished Service Medal during World War I. The citation reads:

"The President of the United States of America, authorized by Act of Congress, July 9, 1918, takes pleasure in presenting the Army Distinguished Service Medal to LTC (Signal Corps) Joseph O. Mauborgne, U. S. Army, for exceptionally meritorious and distinguished services to the Government of the United States, in a duty of great responsibility during World War I. As head of the Engineering and Research Division of the Signal Corps, LTC Mauborgne rendered conspicuous in connection with coordinating the design and supply of new technical apparatus for the Signal Corps. He was largely responsible for the high type of radio equipment developed for our Army and rendered unusual

service in connection with cipher telegraphy."

When Mauborgne returned home he was a lieutenant colonel.

Mauborgne would return to Europe in 1921 as a participant in the Conference on Electrical Communications. In the early 1920's, Mauborgne published an article in Field Artillery Journal entitled "Radio Communication for the Field Artillery," which basically described the communications structures that would be employed by the field Artillery 20 years later in World War II.

During the 1920s and 1930s he would serve as the commanding officer of the Signal Corps Laboratory in the Bureau of Standards, signal officer for the 9th Corps, and director of the Signal Corps Aircraft Factory at Wright Field.

Mauborgne's experiences in France led him to be concerned about the excessive amount of time needed to encrypt and decrypt messages. So he set about creating a simple, yet secure, machine to accomplish this tedious and time consuming task. Building on a sliding paper strip system idea developed by his colleague CPT Parker Hitt, Mauborgne transformed the strips into a series of 24 rotating metal cylinders mounted on a rod. The resulting apparatus became the venerable U.S. Army Cipher Device M-94 that saw service from its introduction in 1922 until the early days of World War II.

During those busy years, Mauborgne somehow managed to sandwich in a year of study at the Chicago Art Institute in 1922-23. When ordered back to Washington in 1923 he matriculated at the prestigious Corcoran Art Gallery for the next three years. Mauborgne's portraits and

etchings were exhibited in galleries in Washington, San Francisco, and Dayton, Ohio. His work was also acquired by the United States Military Academy and can be found in many private collections.

Recognized as a well-rounded, research-minded officer Mauborgne continued to rise in the Signal Corps hierarchy. He was promoted to Major General and assumed the post of Chief Signal Officer in October of 1937. As Chief Signal Officer Mauborgne would become deeply involved and greatly responsible for the success of two pivotal Signal Corps projects that would be crucial to Allied success in World War II, radar and cryptanalysis. Because both projects were secretive by nature, and he retired just prior to Pearl Harbor, his major contribution to the war effort has been largely overlooked and lost to history.

Mauborgne had long been involved in intercepting and decrypting foreign message traffic. His insightful and intuitive mind had been tackling codes and ciphers since before World War I. During his tour with the 9th Corps he was stationed in San Francisco and, on his own initiative, indulged his fancy by intercepting foreign traffic during his off duty hours. He set up a home built receiver in his basement and searched the airwaves for foreign message traffic.

The Depression was in full swing and at first he bore the cost of the electricity himself. Later he was able to salvage an electric meter from The Presidio and have the cost transferred to the government. Much of the intercepted traffic was copied and sent to Washington where it came to the attention of the world's greatest cryptologist William F. Friedman. Mauborgne had known

the brilliant Friedman since World War I and the two developed a warm personal and professional relationship. Mauborgne was instrumental in bringing Friedman and his wife Elizebeth to Washington in 1921 to work for the Army's top-secret Signal Intelligence Service.

Soon after German troops crossed the border into Poland on 1 September 1939, Mauborgne went to Army Chief of Staff GEN George C. Marshall with a plan to expand and direct the SIS's efforts. In February of 1939, Mauborgne had ordered an all out effort in trying to crack the Japanese "Purple" code being used by both the Imperial Japanese Navy and the Japanese embassy in Berlin. With the German attack the effort took on a new urgency.

At Mauborgne's insistence Friedman dropped all other business and set himself and his team to the daunting task. A young statistician, Genevieve Grotjan, was studying six messages sent in "Purple" on the same day when, on 20 September 1940, she found a repeating pattern. The key to the Japanese most secret code was now in American hands. Many weeks of mind-numbing worked followed until the Japanese codes could be read like an open book. An apocryphal story has it that either Friedman or Mauborgne was giving a top secret briefing about the breaking of "Purple" when he waved his hands at the staff, busy at their desks, and said, "These are my magicians" giving the code breaking operation its cover name of "Magic."

These efforts that would contribute to further codes being broken and given the now familiar names of "Enigma" and "Ultra." The projects' security was as great as that surrounding the development of the atomic

bomb, the Manhattan Project. So secret was the code work that the Japanese and Germans would not change their methods, believing their ciphers and cipher machines were impossible to compromise.

It wasn't until the mid 1970s that the veil of secrecy began to lift just a little. The work of the SIS was kept so quiet that in the Office of the Chief of Military History's massive work, The United States Army in World War II, which devotes several volumes to the Signal Corps, there is but one simultaneous mention of Mauborgne and cryptanalysis. Mauborgne was key to this intelligence effort because he was able to get the manpower and facilities needed. His influence went further because his own contributions and competence in the field were such that he was able to inspire those who worked for him to greater efforts.

The accomplishments of the SIS, while under his direction, had been, of necessity, kept secret until the war had been over for some 25 years. Had this not been the case his name would have been as well known and honored as that of GEN Leslie Groves, the director of the Manhattan Project. Certainly his contribution to winning the war was as great.

While he followed the daily work of the code breakers Mauborgne was also pushing hard on the development of better communications equipment for the Army. He saw that the massive expansion of the military build up would not allow the necessary time to train all soldiers in the leisurely Morse Code and pushed for a wide variety of rapid communication radiotelephone devices and the adoption of frequency modulation radios.

Of particular interest to Mauborgne was the development

of transportable radar units and those small enough to be employed in aircraft. A radar demonstration was held in November of 1939 at Twin Lights, New Jersey, not far from the Army's signal facility at Fort Monmouth. Gathered together were the Secretary of the Army Harry A. Woodring, Army Chief of Staff GEN George Marshall, and the heads of the Army Air Corps and the Signal branch - H.H. Arnold and J.O. Mauborgne. It is hard not to imagine the last two reminiscing of a simpler time when their shoulders were less burdened by rank insignia and they soared above Fort Riley experimenting with the cutting edge of technology.

Standing about a prototype portable radar set they watched as a flight of B-17s was tracked over a 280 mile round trip flight to Montauk Point Long Island and back. The demonstration was such a success that the men threw their full weight behind the development of the SCR-270 and SCR-271 radar sets.

By June of 1940 a set would be operational in Panama and others would arrive in Hawaii around Thanksgiving of 1941 and be operating soon after.

By then Mauborgne was approaching the end of his term as Chief of Signal and the statutory retirement age of 60. It must have been a bittersweet departure for a man who had devoted himself totally, and with great success, to the betterment of the Signal Corps for some 38 years.

Mauborgne left Washington soon after his retirement and moved to a small town near Fort Monmouth, Little Silver, N. J. He was a passable violin player and he successfully turned his mind to the building of the instruments,

(Continued on page 48)

(Continued from page 47)

eventually winning prizes in the 1949 International Violin Making Competition held at The Hague. His love of music and the intricacies of cryptanalysis went hand in hand as the mathematical connection between the two is strong.

The prestigious Distinguished Badge program began in 1884 when the U. S. Army first awarded the Distinguished Marksman Badge. The Distinguished Rifleman and Distinguished Pistol Shot Badges are the highest honor that most military and civilian rifle and pistol shooters can aspire to earn. Little is known of Mauborgne's shooting experience but clues indicate he earned a Distinguished Rifleman Badge before shipping for France. He most likely participated in the National

Matches as a junior officer on the Army Shooting Team in the years between 1907 and 1916. This argument is strongly supported by the National Match schedule of that time and the fact that he wears his badge in a photograph taken in France in 1919. He must have held his time on the range in high regard for in his official portrait photograph as Chief Signal Officer the grandfatherly looking Mauborgne looks at the camera through horn-rimmed spectacles with the left breast of his uniform almost bare, an odd thing for a man with so much time in service and so many honors. Perhaps as a portrait artist himself he realized that "less is more." The only awards and decorations seen in this most important of photographs are two ribbons, one of which is the Distinguished Service Medal, the nation's third highest military honor,



**Woodrow Norris and SSG Jonathan Norris accept the Distinguished Member of the Regiment citation on behalf of their great-great grandfather, MG (Ret) Joseph Mauborgne, at the 2015 Regimental Signal Ball in Springfield, Va.**

and his Distinguished Rifleman Badge. In his own quiet way Joseph Mauborgne was double distinguished.

As he approached his 90th year his health began to fail and he moved to the Atlanta area to be close to his family. On 7 June 1971, the only career officer in the U. S. Army to be a graduate of the Chicago Art Institute, a holder of the Distinguished Rifleman Badge, a legend in the cryptanalyst community, a pioneer in radiotelegraphy, and an award-winning violin maker, passed away at the age of 90. He was interred in Andersonville National Cemetery, his last resting place surrounded by the dead of the Civil War.

By an odd twist of fate Mauborgne's obituary in the New York Times appeared directly below an article describing the burial the same day of Audie Murphy, the most decorated

Soldier in U.S. Army history. The ironic juxtaposition of the reports of these two men, both heroes in their own fashion, cannot be lost on those who know that quiet hard work in the rear is as important to victory as stirring valor on the battlefield.

MG Mauborgne is a member of the Military Intelligence Hall of Fame. He is also known as "The Cubic General."

#### **CSM (Retired) Vernon R. Praymous**

CSM Vernon R. Praymous joined the Army in December, 1980. He served all 31 years in the Signal Regiment. He graduated with a Master's degree from Excelsior College. He also holds a Bachelor's degree in Liberal Arts from Excelsior College and a Bachelor in Communications from the University of Maryland. Command Sergeant Major Praymous' military education includes the Primary

Leadership Course, Primary Leadership Development Course, Basic Noncommissioned Officers Course, Air Assault School, Airborne School, Advanced Noncommissioned Officers Course, Drill Sergeant School, First Sergeants Course, Battle Staff Course, and the United States Army Sergeants Major Academy (Class 52).

His military assignments include: US Army Signal Center of Excellence, Fort Gordon, GA September 2011 - July 2012, Command Sergeant Major and Signal Corps Regimental Sergeant Major (Interim)

- Principal advisor to a 2-Star Level Commanding General, his staff and commanders on matters pertaining to over 70,000 enlisted Soldiers worldwide
  - Primary advocate for enlisted management of the Signal Soldiers
  - Coordinated directly with TRADOC and DA on Signal issues
  - Monitored indoctrination of new soldiers and training for noncommissioned officers.
  - Traveled to various installations to visit Soldiers and organizations, gathering lessons learned, and soliciting feedback on training concerns. Implemented changes to schoolhouse training to develop more realistic and relevant guidance for today's mission requirements
  - Participated in community events and engaged in public speaking in the local area and on several installations
- Regimental Noncommissioned Officers Academy, Fort Gordon, Ga. command sergeant major October 2008 - September 2011
- Responsible for the training and development of six military occupational skills (25B/C/W/L/S/N) and a satellite MOS of 25M at Fort Meade, Md.

- Orchestrated a seamless transition from Advanced and Basic Noncommissioned Officers Courses to Senior and Advanced Leaders Courses respectively
- Single-handedly researched, developed, and implemented the Ray D. Lane Conference Room at the Academy in honor of CSM Ray D. Lane, a highly distinguished command sergeant major in the Signal Corps
- Army Diversity Task Force CSM (Washington, D.C.) command sergeant major, August - October 2008
- Was chosen to spearhead the Army Chief of Staff's diversity directives to ensure the Army as a whole, was dispersed geographically by race, ethnicity, and gender with respect to



**CSM (Ret) Vernon R. Praymous**

- positions, assignments, and promotions. Traveled to over 18 installations in a short period of time to gather data to assist in this diversity research and implementation.
- 160th Signal Brigade, Camp Arifjan, Kuwait, command sergeant major, February 2007 - August 2008
- Led unit in combat with oversight of two subordinate battalions dispersed geographically across Iraq and Afghanistan. Served as chief enlisted advisor to the commander and staff on training, career development, mentoring and care of all brigade enlisted Soldiers. Was assigned as the task force signal command senior signal command sergeant major in Iraq and assisted in training and mentorship of every Signal Soldier in theater. Responsible for the tactical communications network and coordination to coalition forces in support of all communications requirements in Iraq.
- 15th Signal Brigade, Fort Gordon, Ga, command sergeant major, May 2006 - February 2007
- Command sergeant major of the largest Signal and Advanced Individual Training brigade in the Army with oversight of four battalions. Advised the commander on all matters concerning retention, training, morale, troop discipline and administration of Soldiers.
- Implemented a unique training program that provided realistic, sequential, and progressive tactical training for over 5000 service members.
- 57th Signal Battalion, Fort Hood, Texas. Deployed to Victory Base, Iraq, command sergeant major April 2004 - April 2006
- Lead unit into combat with

(Continued on page 50)

(Continued from page 49)

oversight of 4 signal companies dispersed geographically across Iraq and Afghanistan. Served as advisor to the brigade command sergeant major and commander on mission, Soldiers, and training. Responsible for the tactical communications network of the battalion in addition to training coalition forces.

50th Signal Battalion, Fort Bragg, N.C., first sergeant, 82nd Signal Battalion, Fort Bragg, Sergeant Major (S3), June 1999 – March 2004

- First Sergeant of a Mobile Subscriber Equipment Signal Company directly supporting 82nd Airborne Corps. Responsible for equipment and facilities valued in excess of \$15 million. Directly responsible for the morale, health, and welfare of 150 enlisted Soldiers.

- Performed duties of S3 Sergeant Major in preparation for attending the United States Army Sergeants Major Academy. Was selected simultaneously for Command Sergeant Major upon completion of school.

57th Signal Battalion, Fort Hood, Texas, first sergeant, May 1995 – May 1999

- First sergeant of an MSE Signal company directly supporting III Corps and other units throughout the installation. Responsible for equipment and facilities valued in excess of \$10 million. Directly responsible for the morale, health, and welfare of more than 100 Soldiers.

97th Signal Battalion, Coleman Barracks, Mannheim, Germany, platoon sergeant, April 1992 – April 1995.

- Platoon Sergeant in an MSE Signal company directly

supporting NATO forces

CSM Praymous' awards and decorations include the Bronze Star Medal (second Award), Defense Meritorious Service Award Medal, Meritorious Service Medal (fifth Award); Army Commendation Medal (sixth Award)' Army Achievement Medal (eighth Award), Good Conduct Medal (eighth Award), National Defense Service Medal (2nd Award), Iraqi Campaign Medal, Global War on Terrorism Expeditionary Medal, Global War on Terrorism Service Medal, NCO Professional Development Ribbon (fifth), Army Service Ribbon, Overseas Service Ribbon (fourth), Drill Sergeant Badge, Combat Action Badge, Parachutist Badge, Air Assault Badge, German Marksmanship (Scuetzenschur/Gold), and the Bronze Order of Mercury.

CSM Praymous is a member of both the Sergeant Morales and Sergeant Audie Murphy clubs. He has served as the president of the Sergeant Audie Murphy Club at Fort Hood.

He is currently employed with RLM Communications, Inc. ("Team Blue") as the senior program manager which specializes in Information Assurance, Technology, and Cyber Security; Service Level Management Implementation; audio and visual support; and program management and staff support services. Since coming to "Team Blue," he has developed and implemented annual coat drives for veterans, strong support of the Marine Toy Drive donating more than 50 bicycles, monthly donations and physical support to the Golden Harvest Food Bank, and support to a nationwide organization called Feed America. In addition to his

superb leadership, knowledge, and passion, he was responsible for finding and relocating RLM Communications, Inc. to a new location in the Augusta area which saved thousands of dollars annually in rental costs. This new location is more conducive to the Augusta and surrounding area but remains in close proximity to the Fort Gordon community.

He is married to MSG (Ret) Savannah C. Praymous. They have five children.

### **COL (Retired) Joseph J. Simmons IV**

**COL (R)** Joseph J. Simmons IV has served the United States Army and the Signal Regiment with distinction for more than 29 years, including four tours of duty outside the Continental United States.

A native of Muskogee, Okla., COL (R) Simmons enlisted in the U. S. Army on September 11, 1969. He attended Basic and Advanced Individual Training at Fort Leonard Wood, Mo., and was awarded the MOS 12A10 (training combat engineer) and attained the rank of Private First Class. Prior to his enlistment, COL (Ret) Simmons applied and was selected to attend the United States Army Infantry Officer Candidate School at Fort Benning, Ga. He reported for this assignment on June 3, 1970 and was commissioned a Second Lieutenant in the Signal Corps on November 19, 1970 and served continuously until retirement on 1 Dec 1998.

His assignments included: communications-electronics staff officer, Intelligence and Control Systems Group, Fort Belvoir, Va.; platoon leader; assistant battalion S2/3; battalion adjutant and later commander, Company

B, 123d Signal Battalion, 3rd Infantry Division (Wuerzburg, Germany); computer systems analyst, Defense Intelligence Agency, Arlington, Va.; chief of plans, assistant deputy chief of Staff Communications-Elections, Headquarters USAREUR; battalion executive officer, 123d Signal Battalion, 3rd Infantry Division; information systems management officer, Office of the Director, Army Staff for Information Management; executive officer and aide de camp to the director, Defense Communications Agency; commander, 123d Signal Battalion, 3rd Infantry Division; commander, 2nd Signal Brigade (Mannheim, Germany); and commander, White House Communications Agency, White House Military Office (Joint Base Anacostia-Bolling, Washington, D.C.).

As the Commander of the 2nd Signal Brigade, COL (R) Simmons supervised over 2,500 Soldiers and civilians geographically dispersed over thousands of square miles. The brigade was comprised of nine battalions (located in the United Kingdom, Belgium, Netherlands, Germany and Italy) and its mission was to provide strategic, tactical, and base communications support for the entire European Theater.

While in command of the highly prestigious White House Communications Agency from 14 October 1994 to 30 November 1998, COL (R) Simmons was responsible for providing premier global telecommunications support and for operating and maintaining a responsive and secure information systems infrastructure for the U.S. President, vice president, National Security Council and the Secret Service.

Immediately following his retirement from military service,

COL (R) Simmons received a Presidential appointment and was commissioned as a deputy assistant to the U. S. President and director, White House Military Office on 1 December 1998. He is the first retired military officer, who commanded a unit within the WHMO, to receive a Presidential appointment and to serve as the director, White House Military Office. As WHMO director, COL (R) Simmons had managerial and oversight responsibility for all the DoD resources, including 2,200 civilian and military personnel and billions of dollars of equipment. The White House Military Office's mission is to provide operational, logistical and information systems support to the President in his role as Commander in Chief, Chief Executive and Head of State.

Currently, COL (R) Simmons is the president of Simmons Leadership Group, LLC. One of his major concerns entails higher education in America. He says that the improvement of our nation's higher educational experience is contingent on the successful convergence of online digital learning and traditional "brick and mortar" learning.

In conjunction with the Army Career and Alumni Program COL (R) Simmons is working with a major online university and public universities to develop professional certifications for transitioning military veterans and their family members.

COL (R) Simmons' professional education includes the U. S. Army Command and General Staff College (1983) and the U. S. Army War College (1992). He earned a Bachelor of Arts degree in History (Magna Cum Laude) from the University of Maryland, a Master of Science degree in Computer Science from the University of



**COL (Ret) Joseph J. Simmons IV**

Oklahoma and was awarded an Honorary Doctor of Humane Letters from National Louis University. COL (R) Simmons was inducted into the U. S. Army Officer Candidate School Hall of Fame (1996) and is a member of the Phi Kappa Phi Honor Society. His awards and decorations include the Defense Superior Service Medal, Defense Meritorious Service Medal (two awards), Meritorious Service Medal (three awards), Army Commendation Medal (two awards), Army Achievement Medal (two awards), Good Conduct Medal, National Defense Service Medal (with Bronze Service Star), Army Service Ribbon, Overseas Service Ribbon (four Awards), and the Presidential Service Badge.

# Amazing Grace of the Hello Girls

By Steven J. Rauch

Grace Banker (1892-1960), a native of Passaic, New Jersey and a graduate of Barnard College, served her country and the Signal Corps as a civilian telephone operator for the American Expeditionary Forces in France during World War I. Her role as chief operator for First Army headquarters during the St. Mihiel and Meuse-Argonne offensives earned her the award of the Distinguished Service Medal, the only woman to receive that honor during the war.

Grace Banker was among the first group of women, commonly known as the "Hello Girls," sent to France to operate telephone switchboards to support the AEF. On 8 November 1917, General Pershing requested the Chief of Signal to form a unit of 100 women telephone operators who spoke French because he felt they had "unquestioned superiority" over men for that task. Having women operators would also free signalmen for duty at the forward units.

In cooperation with the American Telephone and Telegraph Company, women from across the US were recruited to meet stringent requirements of language, a college education, and an ability to train as a switchboard operator.

The women selected were appointed and took the standard military oath and offered the same privileges and allowances as Army nurses. However, they had to buy their own navy-blue uniforms adorned with Signal Corp insignia from a sole source contractor to distinguish them as official personnel. Throughout the war, 223 women were recruited and trained for this important service.

Because of her previous experience as a switchboard instructor with AT&T, Banker was placed in charge of 33 women of Telephone Operating Unit No.1, which sailed from New Jersey on 6 March 1918. Upon arrival in Paris, the unit was divided into three sections, with Banker serving at the headquarters of the Advance Section in Chaumont sur Haute Marne, which served as General Pershing's headquarters.

Banker and the others spent almost five



Signal Corps telephone operator Grace Banker received the Distinguished Service Medal for her exceptional service ensuring continuous and seamless telephone communications at several AEF headquarters from March 1918 to September 1919.

months at Chaumont as other groups of women operators arrived in France. As the AEF expanded its operations in the front line, more offices were opened. On 25 August 1918, Banker was ordered to the First Army headquarters at Ligny-en-Barrois, about five miles south of St. Mihiel where the First Army was to conduct an offensive. With only six operators working in shifts at this forward location, Banker and her team were immersed supporting the planning for the upcoming operation, which included coding operations to preserve operational security. When the St. Mihiel offensive began, Banker and the other women occupied the switchboards during intense opening artillery bombardment at the front. The Signal

operators faced daily challenges of translating between French, English, and American doughboy French to ensure the important information was passed to the appropriate command.

When First Army headquarters moved to Bar-le-Duc on 20 September, Banker and her operators displaced their operations to a very sparse facility that had been greatly damaged from the fighting. While there, Banker and the other women endured aerial bombardment from German planes, but fortunately none of them were injured. They also suffered during a cold, wet autumn in leaky barracks that often greeted them with no heat after long hours at the switchboards. Banker and the

others suffered more challenges on 30 October when a fire destroyed several barracks, including their own.

In November, Banker was to move with some of the women to a new forward location but the Armistice on 11 November ended all combat operations. After over three months of working 12 to 20 hour shifts, Banker was sent back to Paris where she soon missed the camaraderie of loyalty and hard work at the front. She was then assigned to work for President Woodrow Wilson, who was attending the peace conference. She described this duty as "not particularly exciting." When offered the choice to remain in Paris or assignment to the Army of Occupation at Coblenz,

Germany, Banker chose to leave Paris. While at Coblenz, Banker was presented with the Distinguished Service Medal by LTG Hunter Liggett during a ceremony recognizing her with a citation:

For exceptionally meritorious and distinguished services. She served with exceptional ability as Chief Operator in the Signal Corps Exchange at General Headquarters, American Expeditionary Forces, and later in a similar capacity at First Army Headquarters. By untiring devotion to her exacting duties under trying conditions she did much to assure the success of the telephone service during the operations of the First Army

(Continued on page 54)



Grace Banker, front row, left, and fellow Signal Corps Hello Girls receiving recognition by the Army of Occupation at Coblenz, Germany in 1919 for their work in France during World War I.



Women of U.S. Army Signal Corps Telephone Operating Unit No. 1 upon arrival in Paris, France. Grace Banker is seated in the middle and was in charge of the 33-women unit during the embarkation and voyage to France in March 1918.

# Think you know your Wig-wag from your Semaphore system

By Daniel A. Brown and Steven J. Rauch

This article clears up a common misconception about the Wig-wag and semaphore systems of communications.

Over the past several years, encounters with Signal Soldiers have revealed persistent confusion about the names and application of these two very different visual signaling methods employed by the Signal Corps in the late 19th and early 20th centuries. To a casual or inattentive observer, the systems appear to be very similar, but in fact the only similarity is that they both employ hand held flags. Beyond that fact, they differ in almost every detail.

## Wig-wag

The oldest flag system associated with the U.S. Army Signal Corps is called wig-wag. The name reflects the

concept of back and forth movement as a means of signaling through motion.

Often this system has been misidentified as "wig-wam." (A wig-wam is a temporary arched framework structure overlaid with bark or hides to provide shelter used by Native Americans of the Algonquian language group.)

Wig-wag is the signaling system developed for military field operations by Army surgeon Albert J. Myer prior to the Civil War. He developed this system based on a two element "tap-code" he created for the deaf. Myer's wig-wag system uses one flag for signaling. The position of the flags, left, right, front, represent the numerals 1, 2, 3 respectively and combinations of these numerals are used to convey the message. This method enabled a transmission rate of about three words per minute. (See Illustration #1)

The one-flag wig-wag system used a cotton flag of two, four, or six feet square. The larger the flag, the greater distance it could be seen. The flag pole could be extended to a length of 16 feet using 4-foot segments joined with brass fittings.

It took a strong Soldier to wave a 16 foot pole with a 6-foot square flag on it for an hour or more, especially in wind, heat and probably under enemy fire. During night operations, the flag was replaced with a specially designed kerosene fueled torch, but employed exactly as the flag would be during daytime.

During daytime operations, different sizes and colors of flags were employed based upon atmospheric conditions, such as clouds, haze, blue sky, etc.

(Continued on page 56)

(Continued from page 53)

against the Saint Mihiel salient and the operations to the north of Verdun.

In September 1919, Banker and the others sailed for home after almost 20 months service as Signal Corps operators. Their service had been described as "indispensable" and General Edgar Russel, Chief Signal Officer of the AEF wrote on 12 November 1918:

It pleases me a great deal to say that by your ability, efficiency, devotion to duty, and irreproachable and

businesslike conduct of your affairs, personal and official, you ...have set a standard of excellence which could hardly be improved upon and which has been responsible....for the success of our system of local and long distance telephone communication.

Upon their return from the war, women such as Grace Banker did not receive discharge certificates or veterans status as they were considered to have been civilian volunteers, not members of the military. In 1977 Congress finally passed legislation that recognized their

military service and granted them status as veterans. Those still living received honorable discharge certificates and were awarded the World War I Victory Medal. Grace Banker, who died in 1960, did not live to receive this recognition.

Grace Banker served the Army and the Signal Corps during a critical time when skill and courage were needed. Her leadership, technical expertise, and dedication mark her as a distinguished member of the Signal Corps.

## FLAG POSITIONS OF MYER'S ORIGINAL TWO-ELEMENT CODE\*

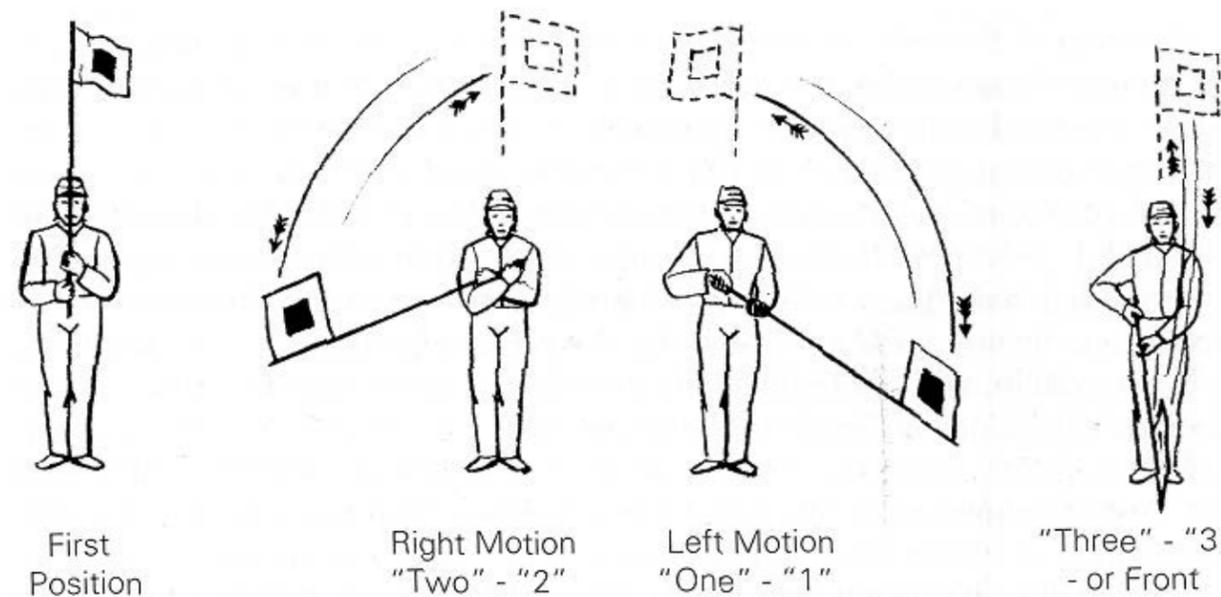


Illustration #1 - Showing the positions of the wig-wag flag during operation. Sources: David L. Woods, A History of Tactical Communication Techniques (Orlando, Fla.: Martin-Marietta Corp., 1965)

(Continued from page 55)

at any one time, only one flag or torch was used for signaling. (See illustration #2)

Confusion about the one flag wig-wag probably stems from casual observation of the branch insignia worn by Signal Soldiers which reflects Myer's wig-wag system in the permutations described.

The insignia illustrates the versatile nature of the wig-wag system

to be employed in all weather and light conditions. Thus the torch and two different color flags are included. (See illustration #3)

The Myer wig-wag system and associated codes were used by both Union and Confederate armies during the Civil War. The Union Navy also employed this system and it served as the first Joint Signal Code between the Army and Navy until the end of the 19th century.

**Illustration #3**

- Branch insignia of the U.S. Army Signal Corps. Source: The Institute of Heraldry, <http://www.tioh.hqda.pentagon.mil/Branches/Signal.htm>

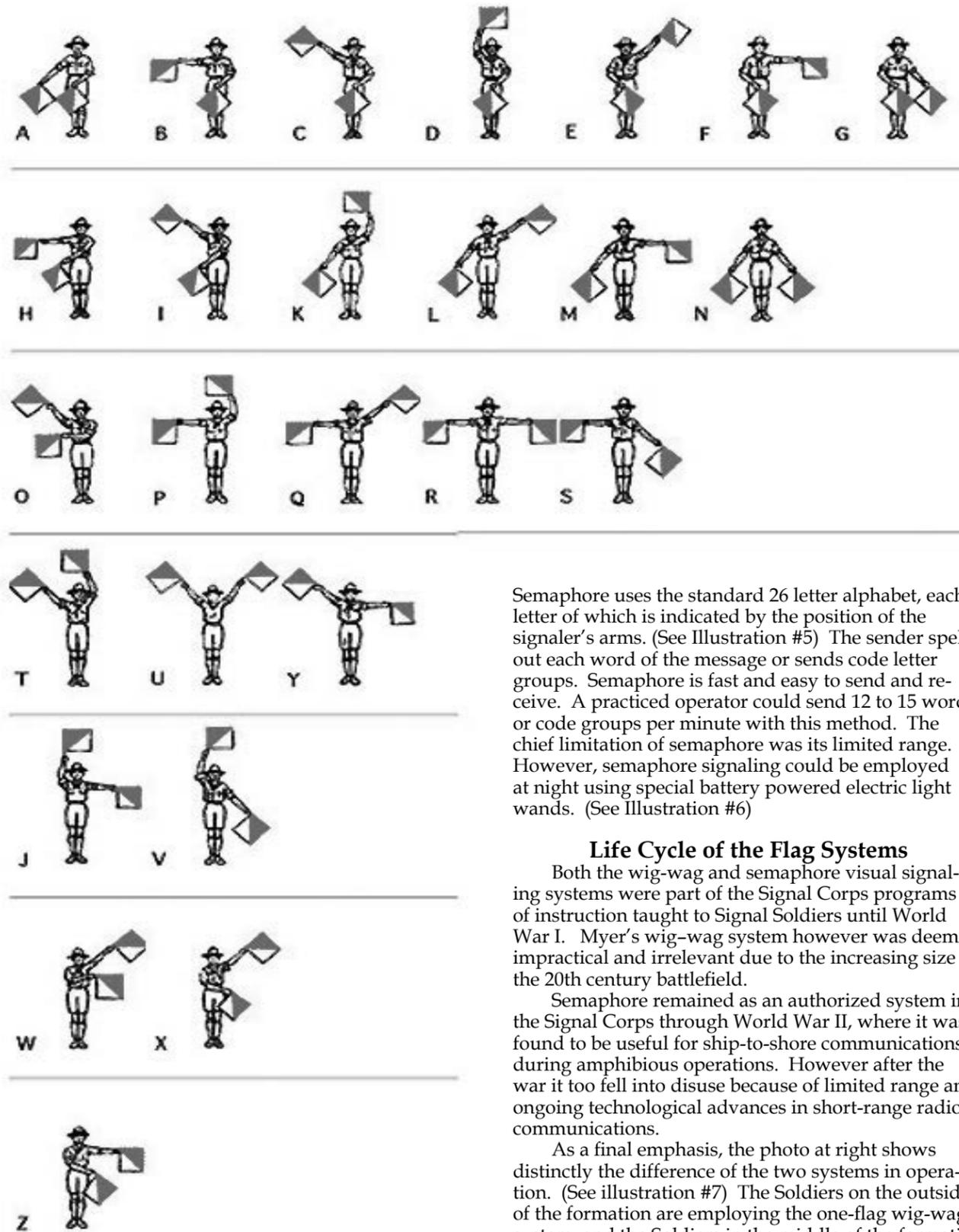


Illustration #5 - The semaphore alphabet

Semaphore uses the standard 26 letter alphabet, each letter of which is indicated by the position of the signaler's arms. (See Illustration #5) The sender spells out each word of the message or sends code letter groups. Semaphore is fast and easy to send and receive. A practiced operator could send 12 to 15 words or code groups per minute with this method. The chief limitation of semaphore was its limited range. However, semaphore signaling could be employed at night using special battery powered electric light wands. (See Illustration #6)

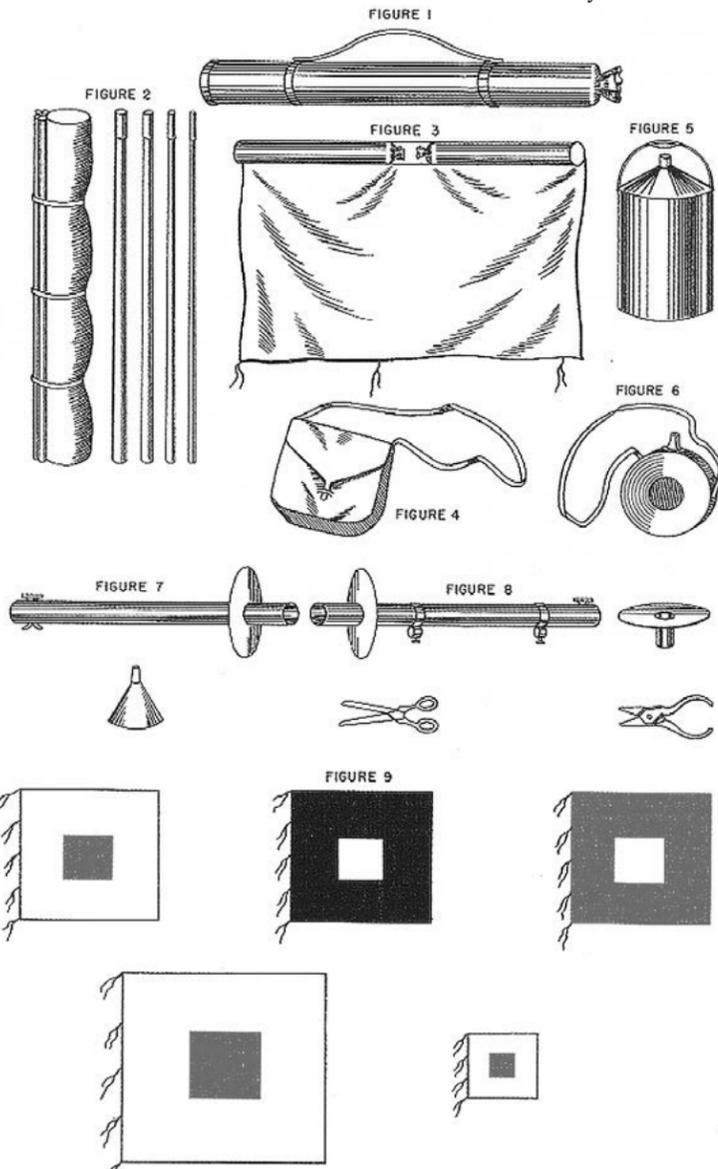
**Life Cycle of the Flag Systems**

Both the wig-wag and semaphore visual signaling systems were part of the Signal Corps programs of instruction taught to Signal Soldiers until World War I. Myer's wig-wag system however was deemed impractical and irrelevant due to the increasing size of the 20th century battlefield.

Semaphore remained as an authorized system in the Signal Corps through World War II, where it was found to be useful for ship-to-shore communications during amphibious operations. However after the war it too fell into disuse because of limited range and ongoing technological advances in short-range radio communications.

As a final emphasis, the photo at right shows distinctly the difference of the two systems in operation. (See illustration #7) The Soldiers on the outside of the formation are employing the one-flag wig-wag system, and the Soldiers in the middle of the formation are employing the two-flag semaphore system. It

(Continued on page 58)



**Illustration #2** - Wig-wag kit with various sizes and colors of flags and torch components. Source: Albert J. Myer, A Manual of Signals: For use of Signal officers in the field (Washington, D.C.: Government Printing Office, 1877).

**Semaphore**

This system of signaling was developed by the Royal Navy for use during the Napoleonic wars. The word "semaphore" is derived from the Greek words sema, "a sign," and phero, "to bear or to carry." A semaphore is any visual system of signaling with an apparatus such as flags, lights, or mechanically moving arms, such as those used to regulate railroads. For our purposes, the semaphore system uses flags at various designated positions of a person's arms. The flag semaphore system of visual communication was not introduced to the U.S. Army Signal Corps until 1914. The semaphore method was deemed faster and simpler than wig-wag and had been used successfully by the U.S. Navy and the Field Artillery branch.

Semaphore is a visual system for sending messages employed by one person using two flags that are held one in each hand. The semaphore

flags used by the U.S. Army were 12 inches square, red and white diagonally divided and attached to a small staff. (See Illustration



**Illustration #4** - U.S. Army semaphore flags. Source: U.S. Army Signal Center of Excellence Historical Collection, Fort Gordon, Ga.

(Continued from page 57)

is hoped this short explanation of the two systems will clear up any confusion and promote informed discussion on this topic.

Mr. Steven J. Rauch has served as the command historian at the U.S. Army Signal Center of Excellence since 2002. He is a retired Army officer having taught military history at the University of Michigan and the U.S. Army Command and General Staff College. He holds a Masters Degree in History from Eastern Michigan University and a Masters Degree in Adult and Continuing Education from Kansas State University.

Mr. Daniel A. Brown came to the Signal Corps Command History Office as archivist/historian in 2005. He was a military historian with the National Park Service for 22 years. Mr. Brown holds a Bachelor of Arts Degree in History from Armstrong-Atlantic University and a Master of Divinity Degree from the School of Theology, University of the South.



**Illustration #6** -Battery powered semaphore electric light wands, circa 1900. Source: U.S. Army Signal Center of Excellence Historical Collection, Fort Gordon, Georgia.



**Illustration #7** - Signal Corps Soldiers practicing wig-wag (outside) and semaphore (inside) flag techniques, circa 1916. Source: U.S. Army Signal Center of Excellence Historical Collection, Fort Gordon, Ga.

# Shaping the Joint Information Environment

*Recent conflicts have shown that U.S. military success hinges upon our ability to leverage and execute decisive joint operations, with the ability to operate freely within the Cyber domain being a key component of this strategy. In order to accomplish this objective, the Department of Defense established the Joint Information Environment framework as part of the Secretary of Defense's DoD Information Network defense strategy.*

By Kitsy Young

*Shaping the Enterprise for the Conflicts of Tomorrow*



(Continued from page 59)

The JIE framework is conceptualized to be a secure environment, comprised of shared information technology infrastructure, enterprise services, and single security architecture. The key objectives of the JIE are the achievement of full spectrum superiority, improved mission effectiveness, increased security and realization of Information Technology efficiencies.

The Defense Systems Information Agency was tasked by the director, Joint Staff to be the technical and implementation lead for the JIE and stood up the JIE Technical Synchronization Office. The JTSO is working across several lines of operation to streamline, consolidate and build the JIE architecture in conjunction with the Combatant Commands, Services and Agencies. Some of the lines of operation include Single Security Architecture, Network Normalization and Transport, Enterprise Operations Centers, Core Data Centers, Unified Capabilities, Identity and Access Management, and the Mission Partner Environment.

"Our focus in JTSO is to shape the JIE in collaboration with the Combatant Commands, Services, and Agencies while maintaining a strategic focus on creating a defendable DoDIN," said COL Daniel Liggins, deputy director, JTSO. "We are also focused on maximizing savings and leveraging the best solutions. Today's warfighters need to be able to operate completely, quickly, and accurately within a Joint Information Environment to be able to successfully complete their missions."

In bringing together the complexities of such a large undertaking, JTSO has been focused on the 20 specified tasks given to them by the JIE executive committee through

its JIE management construct. Chief among those tasks is the development of engineering design solutions that define the 'To Be' solution architectures for the JIE, which align to the JIE lines of operation. To date, more than 500 solution architectures have been approved by the DoD's architecture governance body, the Enterprise Architecture Services Board. Those approved solution architectures are available on the joint staff's warfighter mission area portal site and should be used by the combatant commands, services, and agencies to inform their project objective memorandum strategies. Although JIE is not a program of record, these architectures add rigor to the framework and provide specifications and standards for the department to leverage.

JTSO is in alignment with the DoD Chief Information Officer's top priorities, which includes department wide adoption of Joint Regional Security Stacks, a component of the single security architecture.

"JRSS has been our primary focus in alignment with the DoD CIO's priorities," said COL Liggins. "The JRSS is a system-of-systems designed to centralize and enhance the management, situational awareness and network defenses of the joint and service specific systems. Much progress has been made by the JRSS program office and migration teams in implementing JRSS globally, and we are ensuring those solutions are accurately

depicted in our solution architectures."

Additionally, BG Brian Dravis, the JTSO director, was identified as the DISA lead for the Joint Information Technology Single Service Provider Pentagon initiative, whose mission is to consolidate IT capabilities and functions in the Pentagon. His intention is to fully leverage the solution architectures while executing this complex and challenging undertaking.

Today's environment dictates that we execute as a joint team across all domains, to include cyber. The JIE is the DoD's solution to increasing mission effectiveness and streamlining services within the cyber battle space, and JTSO is the technical and implementation lead helping to shape the way ahead.

*Kitsy Young, an IT specialist since 1989, joined the Defense Information Systems Agency's Strategic Planning and Information office in 2008. Young served as a mission partner engagement liaison producing and executing high-level engagements across DISA for the Director and DoD including the Services, Agencies, and International Coalition partners. Upon transferring to the JIE Technical Synchronization Office in 2013, she became the JTSO knowledge manager, supporting and implementing SharePoint sites, content management, and collaboration. She is also JTSO's strategic communications liaison.*

### ACRONYM QuickScan

**CIO** - U.S. Army Chief Information Officer  
**DoD** - Department of Defense Information System Agency  
**DoDIN** - DoD Information Network  
**JIE** - Joint Information Environment  
**JTSO** - JIE Technical Synchronization Office  
**JRSS** - Joint Regional Security Stacks

# DISA Unified Capabilities advances joint objectives

By Andy Bryczek

The U.S. Army chief information officer and the Defense Information Systems Agency are working jointly to advance the Department of Defense's implementation of Unified Capabilities to realize the joint information environment objective state.

UC is a planned effort to gain mission effectiveness from changing telecommunications and real-time data technologies. It is defined by the DoD Instruction 8100.04 as, "The integration of voice, video, and/or data services delivered ubiquitously across a secure and highly available network infrastructure, independent of technology, to provide increased mission effectiveness to the warfighter and business communities."

In short, leaders in the DoD seek to enable personnel with integrated telecommunications and real-time services using single identity.

### How do Army communicators fit in?

The UC strategy depends on service personnel to orient and respond to their organizational needs for the delivery of telecommunications and real time data services in supporting commanders' missions. The complexity and technical challenge of enabling military telecommunications and real-time data requires the active participation and creative skills of all communications personnel to implement effective and suitable technical solutions within their area of operations.

As a key member of the DoD warfighter and business communities, the Army has led the effort to gain increased effectiveness through the UC Implementation Plan issued in 2013.

DISA relies on references issued by the Army CIO in advancing the state of UC within the DoD. These references include Army Regulation 25-13 "Telecommunications and Unified Capabilities;" the "U.S. Army Unified Capabilities Reference Architecture;" and the "Air Force and Army Unified Capabilities Implementation Plan."

Current UC efforts include the deployment of Enterprise Voice over Internet Protocol telecommunications. DISA has established two Enterprise Session Controllers based on Army specifications. The ESCs are available today and ready to support enterprise-wide VoIP telecommunications. Additionally, the DISA Unified Capabilities Certification Office has approved multiple end-user devices, software products, clients, and network devices for procurement by Army to transition existing Time Division Multiplexing telecommunications to Voice over Internet Protocol.

DISA is supporting projects with its mission partners to transition infrastructure in the continental United States, Europe and the Pacific to UC. The Sensitive But Unclassified IP network SoftSwitch Backbone completed deployment in 2012 and Local Session Controllers and Enterprise Session Controllers have been and continue to be fielded.

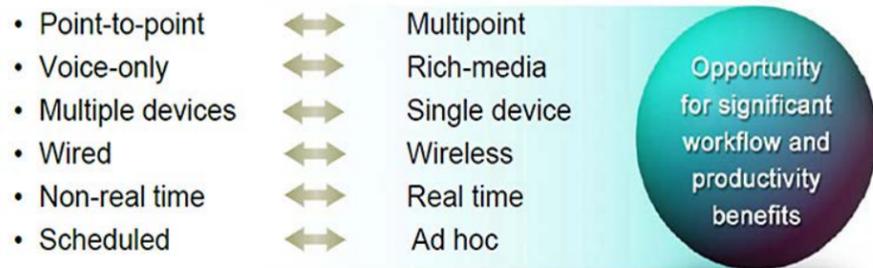
The DISA IP-based SBU voice service designated as EVoIP is accessible over the NIPRNet infrastructure and will ultimately replace DoD's globally deployed 4,025 legacy TDM switches supporting 1,685 sites and approximately 2.7 million DoD and federal agency users on a worldwide basis. Additionally, DISA delivers EVoIP services, helpdesk support, ongoing sustainment, and turnkey installation.

In addition to VoIP, DISA has also deployed Global Video Services and Defense Collaboration Services to support Army users on NIPRNet and SIPRNet.

The GVS provides the capability for users to conduct Video Teleconferences globally either from their desktop/laptop device, as well as from existing VTC centers. User, and center,

(Continued on page 62)

### Changing Technology Drives Evolution



### MISSION EFFECTIVENESS ENABLER

(Continued from page 61)

registration is required for use of GVS.

The application consists of an integrated customer database, a VTC reservation scheduling system, that includes ad-hoc and scheduled conferences, and a resource allocation and management system. GVS supports military organizations in migrating from current legacy TDM video technology and ISDN to an IP-based Global Video Conferencing solution.

GVS enables organizations in achieving their goals with respect to lowering Total Cost of Ownership, improving ease of video services access and rapid deployment, realizing centralized management and

control of network services and resources, increasing operational and maintainability efficiencies, and employing ubiquitous video services access availability, anytime, and anyplace.

The Defense Collaboration System provides the capability for users to conduct web conferencing globally from their desktop/laptop. Additionally, with installation of the DCS Chat client, users can also chat independent of the web conferencing capability. DCS is currently replacing the legacy DCO service. DCS is available to all Common Access Card holders on NIPRNet and all SIPRNet Hardware Token holders on SIPRNet, allowing users to communicate and share information in a secure forum.

DCS WEB Conferencing allows mission partners to be invited in and managed as “guests” for collaboration purposes. For Web Conferences, DCS includes the ability to upload files, converse via audio or text, whiteboard, multiple webcam use, desktop sharing, recording of conferences and store for future use, and over 250 concurrent participants within a conference. The DCS chat client is an Extensible Messaging and Presence Protocol application which provides users enterprise chat client capabilities for quick and easy messaging, communication, and file transfer. DCS employs Public Key Infrastructure authentication resulting in an easy and intuitive login ability with CAC or SIPRNet Hardware Token for users of both conferencing and chat services. Additionally, DCS provides Portable Document Format Support: PDF files can be uploaded and shared without having to convert the PDF to an alternate file format.

DISA workers continue to supporting the Army CIO way forward in the near term for realizing affordable, rapid and effective UC for the Army’s mission and business needs.

### ACRONYM QuickScan

CAC - Common Access Card  
 CIO - U. S. Army Chief Information Officer  
 DCS - Defense Collaboration System  
 DCO - Defense Collaboration Online  
 DISA - Defense Information Systems Agency  
 DoD - -Department of Defense  
 ESC - Enterprise Session Controllers

EVoIP - Enterprise Voice over Internet Protocol  
 GVS - Global Video Services  
 ISDN - Integrated Services Digital Network  
 SBU - Sensitive But Unclassified  
 TDM - Time Division Multiplexing  
 UC - Unified Capabilities  
 VoIP - Voice over Internet Protocol  
 VTC - Video Teleconferences

# Towards the Next Generation Army IT Procurement System

BY MAJ Alexander Vukcevic  
 Michael R. Grimaila  
 and James N. Mark

*In 2013, the Army purchased over \$1.6 billion dollars in information technology equipment from sources other than enterprise procurement vehicles through the Army Chief Information Officer/G6 Goal 1 Waiver system. Of these requests, \$1.1 billion were unable to be categorized in any way, and the remaining \$500 million that could be generically sorted did not provide enough information to reprogram any requests back into an EPV. As the number of waivers continues to grow each year, the Army CIO/G6 seeks to transform the Goal 1 Waiver system to meet the accountability needs of the Army while providing high quality service to the Warfighter.*

**Disclaimer**  
 The views expressed in this article are those of the authors and do not reflect the official policy of the U.S. Army, the U. S. Air Force, nor the Department of Defense.

(Continued on page 64)

(Continued from page 63)

In this article, we present the preliminary findings of our research into the strengths and weaknesses of the existing Goal 1 Waiver program. We then propose a short term method to prioritize requests, discuss the benefits of a unified taxonomy, and explore an automated collaboration solution to streamline the process. This central tool would manage the request process from submission to formal accounting, deliver information to stakeholders, manage digital signatures, and provide decision makers with relevant metrics and analysis.

### Background

Technology is the cornerstone of battle space superiority in the information age, and a decade at war has given the Army a ravenous appetite for IT. In 2010, the U.S. Army spent in excess of \$15 billion on IT related products, programs, and services. We knew the money was spent, but what did we buy? Did our purchases meet Information Assurance requirements? Did we make smart purchases? Are we being good stewards of tax payer dollars? The urgency of war clouded the answers to these questions, and in the years following Fiscal Year 2010 the annual IT budget began to decline. The Army is now trying to maintain the level of IT support it has come to expect at a fraction of the budget. To this end, we study the evolution of the Army IT procurement process, why it isn't working, and propose phased changes that improve mission support while enabling the accountability and visibility required by decision makers and those who will be held fiscally responsible.

Maintaining an IT acquisition system for the US Army is not an easy task. A decade of wartime urgency has made the IT needs of the Army mirror those of a tech giant in the growth phase of its life cycle. Tactical units require tools that show them real time battle space in a package small enough for them to carry. The network enterprise needs constant hardware and software upgrades to feed the growing array of bandwidth hungry end user applications

IT Request	Total Requests	Uncategorized	Uncategorized \$ Requested
Hardware	4171	2448 (59%)	\$129,251,062 (35%)
Software	2738	1683 (61%)	\$62,033,088 (47%)
Services	1727	1135 (66%)	\$916,988,660 (81%)
Testing	38	20 (53%)	\$176,553 (14%)
<b>Total</b>	<b>8674</b>	<b>5286 (61%)</b>	<b>\$1,108,449,363 (68%)</b>

Table 1. Goal 1 Waiver Requests for 2013 (Goal 1 Query as of 2/7/2014)

while continuing to meeting security requirements. As a consequence, the gatekeepers of this system are over tasked and live in reaction mode.

The Army turned to a 'decentralized planning' and 'decentralized execution' model to keep pace with the IT centric needs of diverse and dynamic wartime missions. This model comes with risks. Processes that were once quantitatively managed devolved to barely meeting the Capability Maturity Model base criteria for managed processes.

The regression is most visible in use of EPVs such as Computer Hardware Enterprise Software and Solutions. A unit commander is mandated to use CHES for Commercial-Off-the-Shelf IT needs. When CHES is out of stock, does not support exact requirements, or cannot meet operational timelines, the commander can contract with another vendor. However, these products haven't been vetted through security channels and may not meet Certification and Accreditation standards. This bypass also removes the automated purchasing record that enables budgeting and accounting to easily keep track of the money. For the time, commanders accepted this loss of accountability in order to meet critical mission needs.

In 2010, the Army shifted to a postwar outlook on funding and tried to mend this process to improve accountability and transparency. The CIO/G6 took approval control of local and non-IT budgeted funds through the Goal 1 Waiver system. Since then, Goal 1 Waiver has become the hub for special approval requests, and anything that the EPVs cannot accommodate. Approved Goal 1 requests have grown exponentially since 2010, surging over \$1.6 billion by 2013. A web interface meant to validate a few non-budgeted requests by a small staff is now used to process, analyze, and automate the IT needs of the entire Army.

### Goal 1 Waiver Analysis

In an effort to redirect requests back to the EPVs, we analyzed the waivers in the Goal 1 system from 2013. Upon review of the nearly 9000 IT requests, we found it difficult to conduct a useful analysis due

to the lack of standardization in the information provided for each request. Of the \$1.6 billion in total requests, \$1.1 billion was unable to be categorized in any meaningful way and the remaining \$500 million that could be sorted generically did not provide enough information

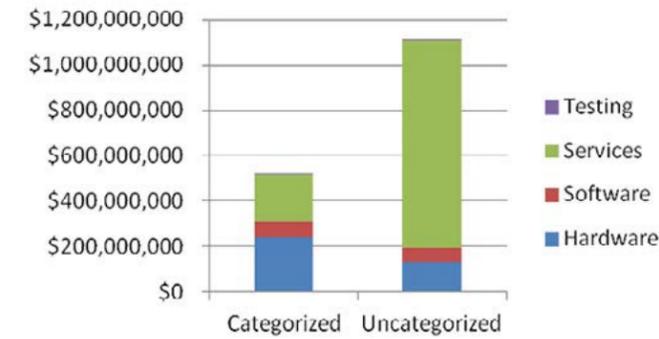


Figure 1. Total 2013 requested IT dollars by 'Item' Criteria (Goal 1 Query as of 2/7/2014)

to be able to reprogram the requests back into an EPV. While the Goal 1 system excels at its primary function of verifying and validating user requests, the automated system is not currently designed to collect decision quality information needed to expedite requests.

The Request Packages that cannot be handled by Army CHES are by their nature varied and unique. The existing Goal 1 menus are built in a way that a request may meet multiple criteria. For example, funding for a system administrator to perform upkeep on an existing SQL server meets three 'Item' criteria and is marked as 'Other.' The requestor then explains the details at great length in the Description field. While the Description field provides the means for the requestor to provide clarification of the need for request, the unstructured nature of the data results in great difficulty when trying to compare competing requests.

In order to understand the magnitude of the problem, Table 1 below shows that in 61% of all 2013 submissions 'Item Type' were marked as 'Other' or left blank. Figure 1 shows that this lack of fidelity resulted in \$1,108,449,363 of non-standard Army IT requests which cannot be sorted at all.

It is clear the Army needs a new system to manage IT requests. In the remainder of this article, we identify the short term needs of IT acquisition

stakeholders, propose near term changes, and propose an automated and sustainable solution.

### Short Term Reform Proposal

In order to remain flexible to new software platforms, we will focus on the general elements necessary for a sustainable IT acquisition process. The scope of this proposal will focus on collaboration for processing requests, and will not address governance issues such as policy, roles, and enforcement. The objectives of this proposal are to:

- Reduce average total processing time for all IT requests to less than 10 days.
- Accurately account for all IT funds spent throughout the Army.
- Reduce the amount of funds being placed on higher cost non-enterprise contracts.
- Maximize cost-effectiveness by empowering EPVs to remain relevant to the customer.
- Enable trend analysis, projections, and dynamic reporting for cost and procurement decision making.
- Minimize the use of non-standard equipment.

Figure 2 shows a modified Joint Capability Area Capability View to illustrate what Capabilities this process uses to enable Enterprise Services, how they align with Army Objectives, and the Activities required to support them. The JCA goal of this process is, "The ability to provide to all

(Continued on page 66)

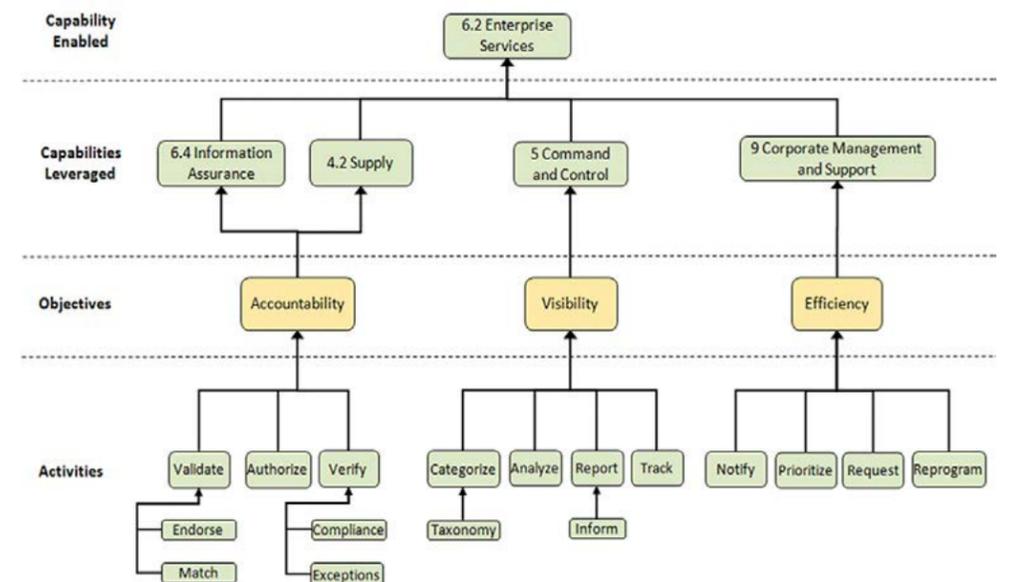


Figure 2. Modified Joint Capability Area (JCA) Capability, Objectives, and Activities View

(Continued from page 65)

authorized users awareness of, and access to, all DOD information and DOD-wide information services.” To accomplish this task, the process must provide Accountability and Visibility using the standards set by Information Assurance, and Army Supply and Acquisition Regulations, while improving acquisition efficiency for the Warfighter.

### **Prioritization**

The existing Goal 1 Waiver interface is a simple, home grown platform. The database receives user input and employs a First-In-First-Out presentation of Request Packages for approval. It does not consider what is in the package or who submitted it. Much like a SharePoint portal, it functions as a repository that requires the user to decide what is important. Before we consider a long term solution the CIO/G6 must be able to sort and address requests in order of their value to the Army. Criteria must be chosen and weighted to score all Request Packages. Based upon a review of Army doctrine, instructions, and policies, we identified the following policy directed criteria as significant:

### **Army Mission Support**

The priorities published in the Army Resource Priority List by the Force Management Directorate tell units how to provide the greatest benefit to the Army. The four ARPL categories are: Expeditionary, Critical, Essential, and Enhancing. These categories would serve as an Army level update and replacement to the Risk Analysis for Army Property guidance.

### **Unit Mission Criticality**

The Army G8 equipping guidance and the annual unit IT transformation plan will drive unit purchasing priorities. These guidelines shape unit level focus, and can be easily categorized in evaluation factors for loss. However, instead of loss, the unit will categorize purchases as: Critical, Essential, Significant, Moderate, and Minor to evaluate the risks of non-acquisition.

### **Asset Replaceability**

Time required to replace an asset is a strong metric when evaluating services that are “Always on.” DA PAM 190-51 uses cut offs of 5, 30, 90, and 180 days, but could be adjusted to meet Service Level Requirements for the broad spectrum of services.

### **Total Cost of Ownership**

Purchase price, lifetime operations and maintenance, and disposal all factor into this value. Current price breaks of \$25,000, \$100,000, \$250,000, \$500,000 and \$1 million appear to be arbitrary round values, but do serve as relevant divisions when evaluated against budgets.

We have identified the following mission relevant prioritization criteria as significant:

### **System State**

This attribute defines the disposition of the IT need: New Acquisition, Life Cycle Replacement, IT Support, Upgrade, Maintenance, and Moratorium. This field would be applicable to all IT purchases, but may not provide priority value in all cases, or could be given temporary value depending on guidance.

### **O&M**

As funding decreases, the Army seeks to outsource Operations and Maintenance of certain functions, in order to focus on our core competencies. The IT contribution to this effort is to shift from purchasing hardware and software we maintain, to purchasing the services of hardware and software. In this vein, the Army can manage the level at which Army owned and operated purchases are favored.

### **Time Sensitivity**

This attribute would carry a sliding weight based on the mission need date. There is risk involved with adding a weight based on user perceived time requirement. However, AR 25-1 directs units to create annual IT transformation plans, which this system would eventually support as an annual unit IT procurement planning tool. The potential for abuse of this field would be mitigated by each of the following fields.

### **Time in Queue**

This attribute would be calculated in the same way as Time Sensitivity, and act as a balance for abuse of the previous field. The longer a request sits in the queue the more weight it receives. When added to the Time Sensitivity date these fields enable low priority requests that wait patiently at the bottom of the queue to be purchased in time. This is an incentive for commands to plan their purchases early, as they are more likely to have their requests approved by the time they need their equipment.

### **Scope**

Scope addresses the breadth of Soldiers, and civilians,

impacted by the Request Package by considering who benefits from the purchase: Single Organization, Multi Command, Multi Installation, Army Wide, Joint, or Multinational. Scope accounts for technology such as ‘Big Voice’ which has a broad user base, but might not score highly on Army Mission Support.

### **Command**

All commands in the Army are not created equal. The CIO/G6 would weight commands based on senior leader guidance. Much like Scope, the greater area of influence will be taken into account.

### **Commander’s Flag**

The current FIFO system has created a condition by which General Officers are calling the CIO looking to advance their critical purchases through the line of requests. If analyzed and weighted correctly, the above criteria should eliminate the need to bypass the system. However, the Commander’s Flag acts as a mechanism for the GO to push a request to the front of the line by digitally signing this field. The Flag would hold an additive value equal for each command, meaning two requests with Commander’s Flags would move to the front of the line in order of their original weight. GOs would not be able to delegate this request signature authority, and be held accountable to the CIO/G6 for each use, giving this field a low potential for abuse.

The list above could be weighted in many different ways to yield a single prioritized list. While our proposed formula this beyond the scope of this paper, stakeholders in this process must determine the category weights for this system to work.

### **Unified IT Acquisition Taxonomy**

Once prioritization is in place, the terms should serve as a starting point for the development of a Unified IT Acquisition Taxonomy for fixed, concise, and relevant fields. These fields will enable visibility through analysis, trend projections, grouping, and seamlessly transfer data to budget and finance systems. Common language decreases processing time and accelerates long term collaboration. A Unified Taxonomy requires input from Army elements beyond the scope and authority of this research. Below are recommendations for starting points.

### **Business Function Attributes**

Business Functions are fixed “big picture” fields, not directly related to the IT need. These fields focus

on administration: Requesting Command, Scope, Purpose, Management Decision Packages, and Army Program Elements, etc. If an IT Asset doesn’t have its own discrete selection within the larger Request Package the CIO/G6 must determine a way to separate them, or accept the multiple selection criteria for the given field. These values should aim to be discrete, “pick one” drop-down menus.

### **IT Need Attributes**

IT Needs should be “pick one” in broad IT categories and “pick all that apply” for Bins dealing with the specific equipment. For example, Tier One may consist of: Tactical, Data Center, Office, or Infrastructure. Tier Two may be a short list of device types. Tier Three, where unit requirements become unique, provides check boxes of all unique fields previously requests. Tier Four will provide a short answer ‘Other’ section to allow growth in Tier Three. In a short time the CIO/G6 could build a relevant and accurate Third Tier comprehensive enough to only see ‘Other’ with emerging technologies.

### **Finance Centric Taxonomy**

During this research, we examined the Air Force and Navy IT procurement systems. The Air Force currently operates in a similar decentralized system to the Army. The Navy, however, has consolidated their ‘non-weapon system’ IT procurement into the Navy Information Dominance Approval System.

The intent and scope of this contracted system are similar to those of the Army. NAV-IDAS functions as intended, but does not account for naval financial systems. The Navy currently faces the challenge of tying requests to funding. The Army has an opportunity to learn from this challenge by integrating the Army Portfolio Management Solution and the General Fund Enterprise Business System into the early stages of process restructure.

By building an IT procurement tool with budgeting and accounting at its core, the Army would maximize its ability to build a fully integrated collaboration tool, while priming it for migration and consolidation into the financial core at any point in the future.

### **Long Term Collaboration and Automation**

Once the restructuring of the existing waiver system is complete, the focus would turn towards modifying the system implementation in order to

(Continued on page 68)

(Continued from page 67)

improve the overall efficiency of the process. Figure 3 shows the existing “as is” and the proposed “to be” architecture for the Goal 1 Waiver system. Army IT procurement is currently a cumbersome process. Requests are processed via email in changing formats depending on the destination, and tracking is done by phone.

By building an automated collaboration dashboard units could track their request from start to finish in one place. The dashboard would provide real time tracking updates for all Request Packages, to include individual IT Asset progress through the system.

When a stakeholder finishes their action the dashboard would route the request to the next stakeholder and generate an email notification for action.

Units would be able to see the current action owner, for how long, what actions others have taken, and comments in a format

that could be briefed directly from the interface. Finally, stakeholders could customize their interface options, allowing them to arrange and display data in a way that best suits their needs.

Formatting changes would be transparent between stakeholders, allowing the DOD CIO to query and review a request without the Army investing man hours in document conversion.

### Army Service Broker

To further improve the efficiency the Army would be best served by consolidating all IT service contracting. The Army Service Broker would be responsible for all existing contracts and become the negotiator for any new services with agencies such as the EPVs and the Defense Information Systems Agency. Army level management is not required for all service requests, but an Army Service Broker should evaluate and consolidate Army level contracts when

possible.

### Software Platform

The most efficient software solution would be to contract with a provider that has experience with this need and to build the dashboard into an existing Army funded platform. The robust infrastructure of the Army financial platforms would be ideal. As we saw with NAV-IDAS, integrating IT acquisition into Army financial processes at the start will improve efficiency, and mitigate future integration issues.

### Streamlined Purchase Process

In this section, we walk through the general use of this system from submission to acquisition. First, we address the stakeholders in the “Happy Path,” which is a Request Package and associated IT Assets that require no intervention and moves directly to purchase. Then, we discuss stakeholders that become involved in the exception process.

The full work flow diagram for this process is included in a proposed CONOPS document, but contains too many scenarios and routing activities for inclusion in this article. This process is the intended end state for this stage of the system and looks to field no less than 90% of the IT requests submitted by the Army.

### Request Packages

Each submission is considered a Request Package that may contain a variety of IT Assets needed to accomplish the mission. The Request Package as a whole must be approved prior

to the purchase of any IT Assets contained within.

This dashboard would help units meet the Army standard of submitting their annual IT transformation plan by loading projected purchases into the system.

Units would be rewarded for long term planning through the priority weighting criteria. Though pricing and availability fields may become stale over the year, they offer reference for planning and eventual purchase. Once mature, the submission menu should provide units with an exhaustive selection tool that eliminates the need for external document attachment.

### Army Portfolio Management Solution

APMS provides value to this system by integrating resource planning data. Units can use their own projections to guide their requests and determine how much money they should spend, and through which funding streams, all in the interface they use to submit requests. APMS authorization will be a largely automated process. APMS will not have the authority to reject a submitted Request Package from being processed.

If a request is not associated with a funding code APMS will merely annotate the unfunded requirement for stakeholders in the unit’s chain of command to make a determination.

### Enterprise Procurement Vehicle

Relevant EPVs would review the IT Assets in the package and determine what they can and cannot provide, and at what price. The disposition of each IT

Asset would then be annotated within the Request Package in the Dashboard. Like AMPS, the EPV will not stop a request whose requirements it cannot fill. Rather, it will send the IT Asset back to the requestor for an addendum of vendor quotes to be added to the request. The dashboard will only forward the total Request Package on to the Command once all required IT Asset information has been added.

### Command

Once all budgeting and availability details are gathered, the requesting unit’s command would decide whether or not to approve the request. If the Command rejects the Request Package the request would remain in the system as a value added data point with the reason for rejection. The rejected request is available in the database for analysis, and if the Command wishes to approve the request at a later date the process can easily resume.

### Higher Command

The request then goes to the higher Army Command, Army Service Component Command, or Direct Reporting Unit for approval. If the Request Package and its IT Assets are fully funded the command would digitally sign and forward to GFEBS. If unfunded exceptions exist, this will be the first level of divergent action in the Exceptions sections below.

### General Fund Enterprise Business Systems

Once all IT Assets in the Request Package are approved GFEBS commits and obligates funds, then routes the request

to the appropriate contracting office.

### Exceptions

In this section, we discuss Request Package gatekeepers and IT Asset sorting for exceptions. This section represents a direct change to the existing Goal 1 Waiver process, which will now become a component of the larger request management system. Figure 4 depicts the proposed workflow for the process.

### CIO/G6

The primary function of the CIO/G6 is to review exceptions for IA compliance, and conduct analysis on IT Asset exceptions that aren’t being addressed through EPVs. At full system maturity the CIO/G6 should focus primarily on trends, projections, and contract forming with the Army Service Broker.

### DOD CIO

The DOD CIO only enters this process for IT Asset requests that require DOD approval, such as moratoriums and specified purchase restrictions.

### Hardware

The hardware approval process will remain unchanged. Request specifications will be reviewed and annotated for unique requirements that are not being met by EPVs, then approved if there are no compliance issues. Hardware may prove to be the hardest IT Asset category to standardize, and could maintain a long term place in the Exception process.

### Software

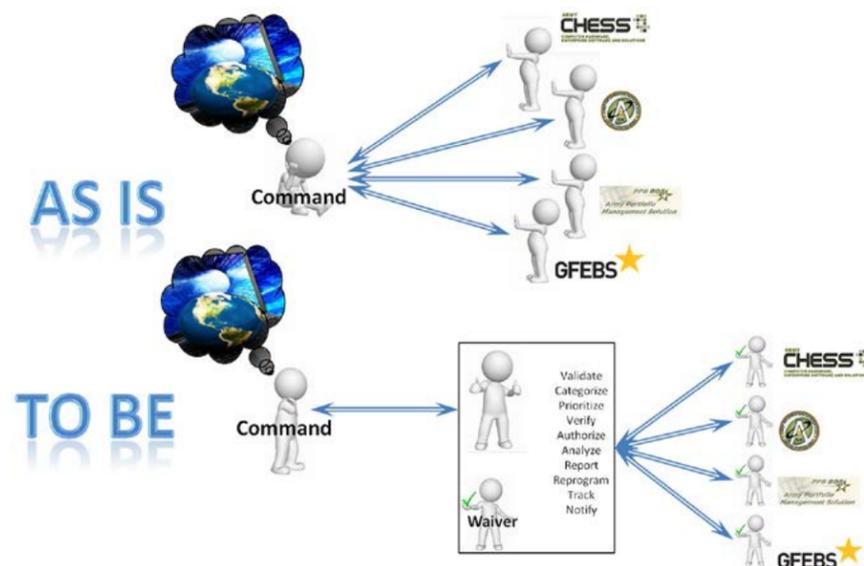


Figure 3. Process Concept Change

(Continued on page 70)

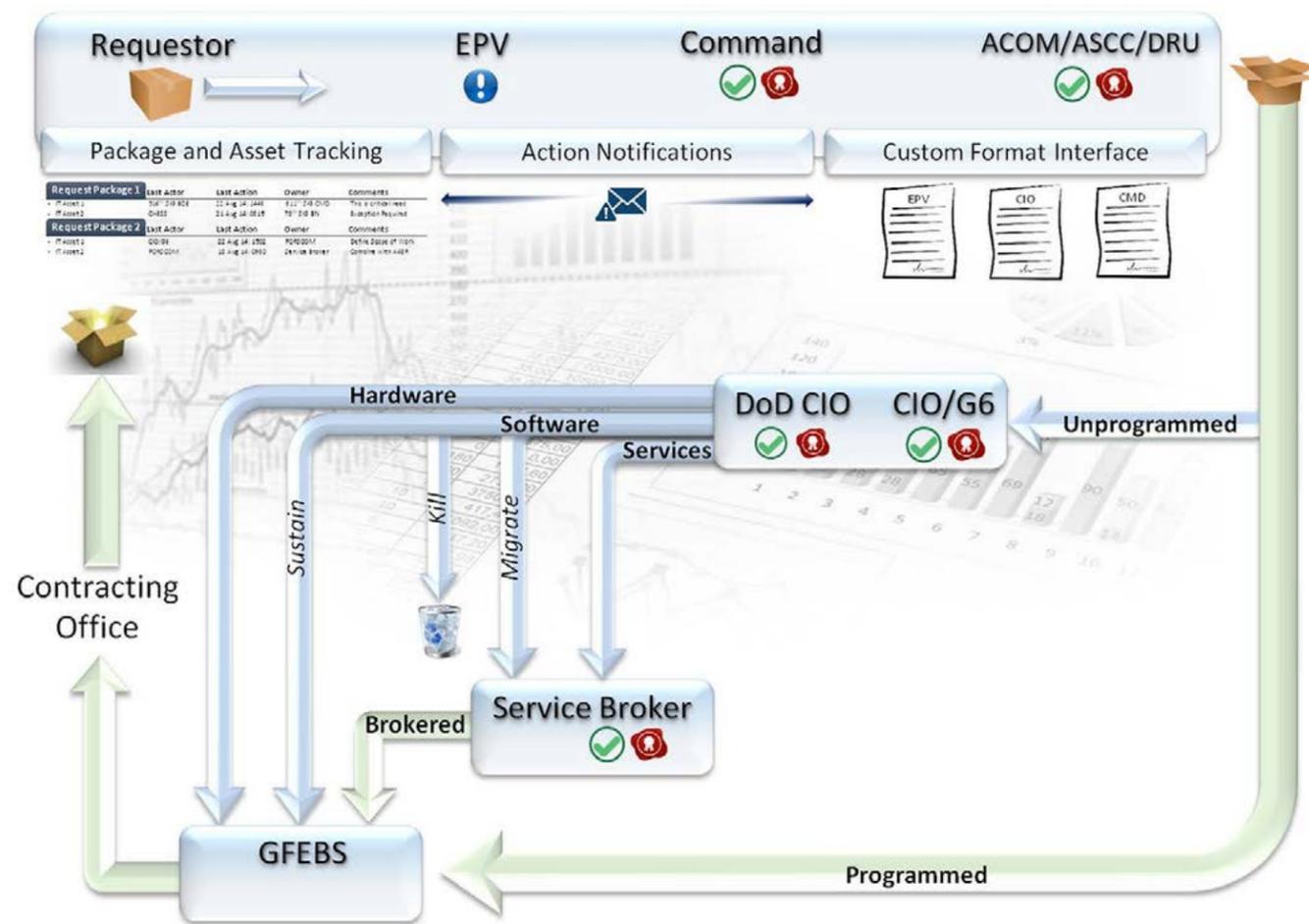


Figure 4. Proposed Work Flow

(Continued from page 69)

The Software Exception process would be subject to the Army Applications/Systems Migration – Rationalization and Disposition Process. If the software meets the requirements of the modernization checklist it will be forwarded to the Army Service Broker for processing. If the software is determined to be temporarily sustained, short term licenses may be issued. If the software meets no requirements, the Request Package will be rejected until the software is removed or modified.

#### Army Service Broker

The Army Service Broker would become the gatekeeper for contract services which would accelerate the Army’s intended migration into the cloud. The Army Service Broker would work closely with the CIO/G6 to determine what contract modifications would be of the most benefit to the acquisition process.

#### General Fund Enterprise Business Systems

Once all exceptions in the Request Package are addressed the Request Package is approved. GFEBs commits and obligates funds, then routes the request to the appropriate contracting office.

#### Analysis and Reporting

This consolidated process provides its greatest value to the Army in the form of IT metrics. Through real-time analysis the Army will be able to customize and automate financial accountability, trend analysis, program threshold triggers, value mapping, and any other analysis requirement that may arise in the future.

#### Financial Accountability

This system would serve as the connecting interface between APMS budgeting and the GFEBs spending until a long term integration solution

could be agreed upon.

#### Decision Analysis Tools

The CIO/G6 would be responsible for analyzing the database, but they would not have to build their tools from scratch. The Armament Analytics Multiple Objective Decision Analysis Tool is Value Based Analysis tool designed for weapon procurement that could serve as a model for finding further efficiencies in IT procurement process.

#### Trend Analysis

Trend analysis would enable the CIO/G6 and the Army Service Broker to make data driven decisions when negotiating EPV contracts. With enough trend data the CIO/G6 would be able to project when a program would need to be established, and set threshold triggers in the system that would provide an alert when criteria is met. In addition to common metrics, the CIO/G6 could to easily combine fields to generate new information without any modification to the

system.

#### Value Mapping

As the database grows, priority factors will begin to trend in correlation to their total cost. This would eventually yield “soft” upper and lower limit bands for normal purchases. This value map could provide a guide to determine the cost effectiveness of any given request. This would not be hard cut off, but rather additional information for decision makers to consider when presented with a Request Package. Figure 5 shows a value mapping example which provides a cost versus priority view of requests. Such a figure provides decision makers with a visual understanding of requests to support decision making.

#### Total Integration

The development of IT procurement tools based on collaboration, automation, and consolidation has long term implications for how the Army allocates funds, spends, and balances its budget.

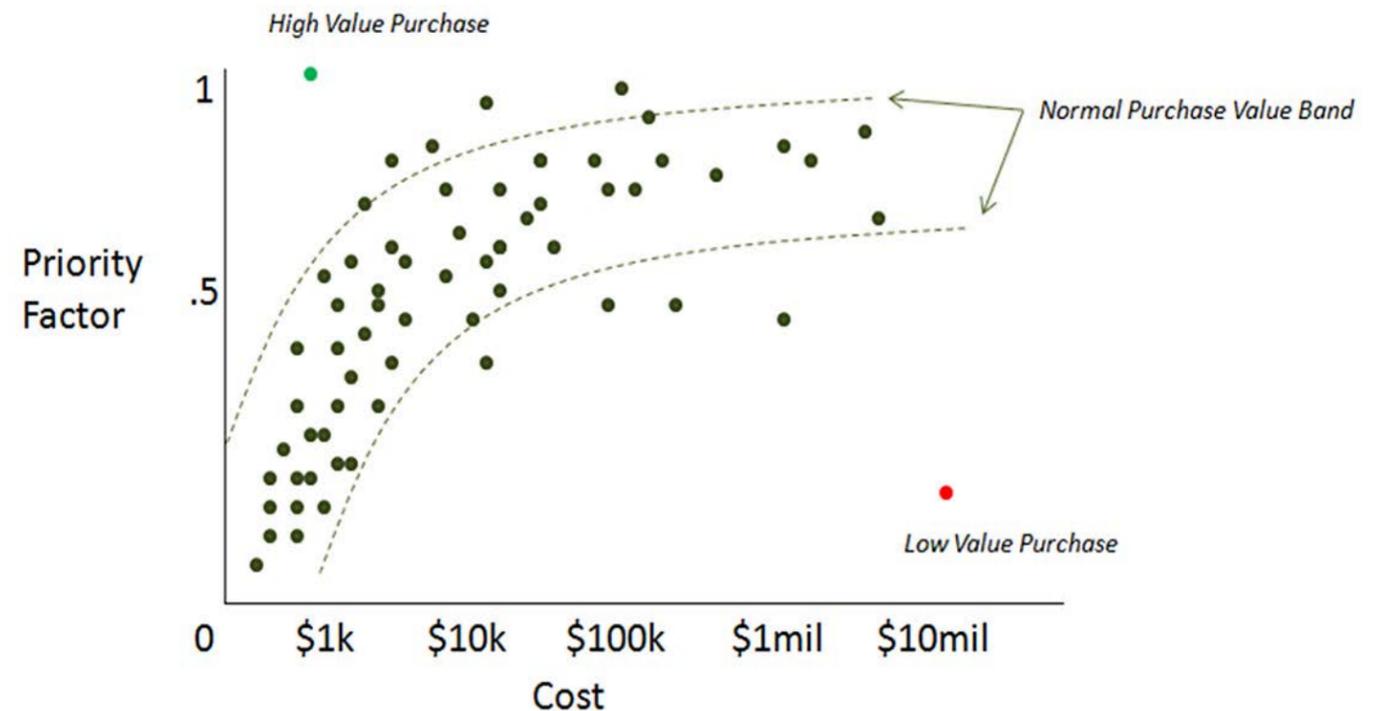


Figure 5. Value Mapping Example

(Continued on page 72)

(Continued from page 71)

By continuing to integrate the Army purchasing and funding process becomes a Wiki of information, giving stakeholders access to all mission relevant content through a single interface.

### Conclusion

In this article, we discussed the IT Acquisitions challenges facing the Army brought on by a decade of war. We proposed a possible course of action for prioritization and a Unified IT Acquisition Taxonomy. This course of action would lay a foundation for the Goal 1 Waiver system to migrate into an automated collaborative dashboard. This dashboard

would provide the Army warfighter with a streamlined IT acquisition process from submission to delivery. Beneath the dashboard, the central repository would allow the CIO/G6 to track requests, manage digital signatures, conduct analysis on purchasing trends, establish thresholds and projections, automate financial reporting, and provide decision makers with relevant metrics in real time. By building these tools into the Army financial platforms and working back towards the IT needs of the warfighter, the Army can realize a sustainable solution for efficient, accountable, and visible IT procurement.

*MAJ Alexander Vukcevic is a Functional Area 24, currently enrolled in the Masters of Engineering Management program at the Air Force Institute of Technology.*

*Michael R. Grimaila, PhD, CISM, CISSP is a professor and head of the Department of Systems Engineering and a member of the Air Force Cyberspace Technical Center of Excellence (AF CyTCoE) at the Air Force Institute of Technology.*

*James N. Mark, MA, MBA, MSCE is the ARFIT and Goal 1 Waiver Program Lead within the IT Investments Division of the HQDA CIO/G6.*

[Join the Discussion](#)

<https://SIGKN.army.mil>



### ACRONYM QuickScan

APMS - Army Portfolio Management Solution

ARPL - Army Resource Priority List

ARFIT - Army Request for Information Technology

CIO - Chief Information Officer

CHESS - Computer Hardware Enterprise Software and Solutions

DOD - Department of Defense

FIFO - First-In-First-Out

GFEBs - General Fund Enterprise Business System

GO - General Officer

EPV - Enterprise Procurement Vehicle

FY - Fiscal Year

FIFO - First In First Out

IA - Information Assurance

IT - Information Technology

JCA - Joint Capability Area

NAV-IDAS - Navy Information Dominance

Approval System



# Fielding Ready Signal/Cyber Teams

BY MG John W. Baker

*The fact is if you can't communicate in our Army, you can't command, put steel on target, or defeat our enemies.*

## Forward deployment and rotational force presence advantages

A former commanding general I worked for would often tell me “If we’re not communicating, then we’re just camping!” It is the business of our Service Cyber Protection Teams and Signal formations to provide warfighters the communications networks required to ensure mission command.

The Army has a significant

**“If we’re not communicating, then we’re just camping!”**

role in maintaining the base of the Department of Defense Information Network which ensures mission success. Our role is to work with our Service partners and allies to maintain our theater and global networks. Within this role our Army has tremendous opportunities. Our Services’ leadership are strong advocates for the continued

forward deployment and rotational force presence of Service Cyber Protection Teams and Signal formations and Soldiers in support of our military engagement strategy and contingency planning. It makes sense to provide these opportunities to acquaint our leaders and units with the complex issues of building and maintaining our complex networks around the globe. While competition for dollars is intense in our fiscal environment, this approach brings balance among competing interests. This balance is achieved by ensuring the Army’s participation in a joint and whole-of-government approach to maintaining our global networks. Leadership and speed matter when responding to network challenges; and none are better than Army cyber professionals and communicators. This approach, a combination of forward deployed Service Cyber and Signal forces and rotational forces, allows an adaptive, creative, flexible, visible presence which can build confidence and trust with our partners around the world while presenting and preserving options for our Army units and Combatant Commanders.

This combination of forward deployed forces and rotational Service Cyber and Signal forces is a tremendous opportunity allowing leaders and units to acquaint themselves with the complex issues of different areas. It establishes and maintains relationships while deepening theater security cooperation thru participation in exercises, planning conferences, seminars, and training events.

A continuous rotational presence of Service Cyber Protection Teams and Signal forces would enable different units to gain experience training with our forward deployed units and allies. This approach facilitates the focus of Army home station training and Combat Training Center rotations. During home station and preparation, detailed analysis and instruction can be conducted on the area of responsibility. At the CTCs, the Joint context for training across warfighting functions can be emphasized.

We must converge network expertise in cross-domain, multi-domain warfare involving air, cyber, land, sea, and space. With our Joint

force partners we should focus on integrating our Army network capabilities to assist Combatant Commanders in deterring conflict, compelling adversaries, and shaping the outcome.

### Applying years of Lessons Learned

Forward and rotational Service Cyber Protection Teams and Signal formations apply lessons learned from 13 years in combat to maximize time, space, and trained personnel and teams, all while strengthening readiness. Since the 1950’s, over 50 countries have hosted at least 1,000 American troops on their soil. Currently the U.S. military has personnel in about 150 nations. We have codified this initiative for forward deployment, rotational presence, and regional alignment within the Army’s new operating concept published in 2014. This initiative, promulgated in the operating concept, makes a compelling case for land power, including Service Cyber and Signal forces, applied with the skill, speed, and precision demanded by our leadership and countrymen. The concept recognizes that deterring enemies and reassuring allies alike requires sophisticated expeditionary maneuver and joint combined arms operations, all linked through Army and joint networks.

The ever-increasing demands of a smaller Army translate into increased risk for contingencies and war plans. We cannot build a relationship on the day we need it. This capability helps develop relationships built on respect. These relationships demonstrate credible network capabilities and genuine leadership provided by Army cyber professionals and communicators. And, we can afford this deterrent ability. The credible threat of military force is a fiscal priority requiring a necessary military deterrent.

The truth is our involvement in current wars is not coming to an end. The variety of potential entanglements emphasizes the importance of our Army’s support to our Nation’s global networks. We face an existential threat from a boxed-in,

(Continued on page 76)



Headquartered at Fort Gordon Ga., 7th Signal Command (Theater) provides Army Enterprise Network capabilities in the Army North and Army South Areas of Operation. The command is one of five theater Signal Commands worldwide, and is a subordinate element of NETCOM/9th SC (Army) at Fort Huachuca, Ariz., and Army Cyber Command at Fort Belvoir, Va.

The command currently operates 37 Network Enterprise Centers providing information technology services at installations throughout the Continental United States. The 106th Signal Brigade commands NECs in the western United States and the 93rd Signal Brigade commands NECs in the eastern U.S. The 21st Signal Brigade performs a wide range of information

technology missions in support of the National Command Authority, operates strategic satellite facilities, and provides direct support to Army South. Two theater-level Network Operation and Security Centers perform technical tasks that enable the command to monitor, manage, and defend the network.

(Continued from page 75)

nuclear-capable Russia. We may be in for a millennial contest with China. If Iran gets nuclear weapons, transferred then to a third party, invaded its neighbors, or increased its support for terrorist groups, the United States would be compelled to respond. It is only a matter of time before North Korea can place a nuclear warhead on its missiles and produce missiles capable of reaching the United States. Dangers from alternatively governed and ungoverned spaces in places like Syria and Yemen continue to multiply.

To paraphrase former Joint Chiefs Chairman ADM Michael Mullen, the Army is the center of gravity for our Department of Defense, thus the Army's networks are the base of the Department of Defense Information Network. If an Army network fails, the Department of Defense Information Network is placed at risk. Forward deployment and rotational Service Cyber Protection Teams and Signal presence are vital elements of our combatant command country plans because they outline a concept of Service Cyber and Signal engagement necessary in today's technology-driven battlespace.

Our forward deployed Service Cyber and Signal elements and rotating forces can lend clarity to future network events while developing credible, genuine,

respectful relationships with our Service partners and allies. Our Service Cyber and Signal units lend adaptability, creativity, and flexibility to the Department of Defense Information Network. In today's networked environment, leadership, speed, and quick reaction matters tactically, operationally, and strategically. Our Services' visible Cyber and Signal formation presence in times of crisis and peace can help give advantage and instill

***Forward deployment and rotational Service Cyber Protection Teams and Signal presence are vital elements of our combatant command country plans because they outline a concept of Service Cyber and Signal engagement necessary in today's technology-driven battlespace.***

confidence in all.

Our Army's Cyber and Signal units as integral members of the combined Services' team continue to assist in our Army's maintenance of the Department of Defense Information Network through forward deployment and rotational force presence. Readiness built over time, balanced with deployments and presence, is a credible, fiscally prudent, and viable deterrent option and strategic necessity. It answers the question of "Where's my ready Cyber Protection Team and Signal force?" during times of crisis while simultaneously providing options.

*MG John W. Baker is the 7th Signal Command (Theater) commanding general. He was promoted to his present grade on July 7, 2015.*

*MG Baker graduated from Norwich University in 1985, receiving his commission as a second lieutenant. He earned Master's degrees from Central Michigan University and the Industrial College of the Armed Forces. He is a graduate of the Armor Officer Basic and Signal Officer Advanced Courses, Command and General College, and Industrial College of the Armed Forces.*

*He has served in a variety of staff and command assignments in Germany, Washington, D.C., Florida, Georgia during his 30-year Army career including deployments to Iraq.*

## Submit an article to *The Army Communicator*

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

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

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

### *How to submit an article*

Steps involved in submitting an article to AC are outlined following:

Select a relevant topic of interest to the U.S. Army Signal Regiment / military information-technology community. The topic must professionally develop members of the U.S. Army Signal Regiment.

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

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

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

OFFICIAL BUSINESS  
ISSN 0362-5745

# Distinguished Members of the Signal Regiment

On March 27, 2015, a Signal Ball was held in Springfield, Va. During the event, eight very deserving people were inducted as Distinguished Members of the Signal Regiment.

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

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

LTG Robert Ferrell presented the awards to: Brigadier General (Retired) Velma (Von) L. Richardson, Colonel (Retired) Joseph J. Simmons IV, Major General (Retired) Joseph O. Mauborgne (posthumous), Command Sergeant Major (Retired) Vernon R. Praymous, Chief Warrant Officer Five (Retired) Leslie E. Cornwall, Mr. David Kintner, Ms. Grace Derby Banker and Major Edward J. Murphy (posthumous). Accepting the awards for MG Mauborgne were his his two great-great grandsons, SSG Jonathan Norris and Mr. Woodrow Norris.

