

ARMY COMMUNICATOR

Voice of the Signal Regiment

PB 11-13-4 2013 Vol. 38 No. 4

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

United States Army

NETWORK OPERATIONS

PLUS:

- *Expanding NETOPS into The Cloud*
- *GEN Robert Cone says company commanders key power brokers*
- *“Active Shooter” offers Joint operations protection*



Chief of Signal

MG LaWarren V. Patterson

Thanks to a great Signaleer

Signaleers,

LTG Susan S. Lawrence recently retired after 41 years of military service. During her career, she held the ranks of private and three-star general and was the first woman to be the Army Chief Information Officer/G6.

She oversaw one of the most dramatic communication upgrades in the Army's history. She spearheaded the installation as a docking station - first tested last year at eight Army posts. This pilot program allows units to connect their SIPR command and control equipment to an installation's secure network infrastructure.

This accomplishes two goals: Soldiers can train on SIPR command systems while in garrison and reduce costly satellite use.

She led the migration of Army email users from scattered exchange servers to a centralized, cloud-based email service operated by the Defense Information Systems Agency. You have to be one smart person to squeeze \$500 million in savings from email.

She projected another one billion in savings by 2015, by further

consolidations and increased shared services.

Her career as a Signaleer has taken her to Europe, Korea, Southwest Asia and across the United States. She has commanded at every level from platoon to Army Signal command.

She has been the epitome of a mentor, coach, teacher and friend to so many in our Signal Regiment and our Army. She also joins a select few as a Distinguished Member of the Signal Regiment.

I have been honored to serve by her side and will never forget her great accomplishments, her unequivocal contributions to the Signal Regiment and most importantly, her continued friendship.

As the sun sets on LTG Lawrence's military career, it is a new dawn for her civilian life. She plans to

continue supporting the Army as a volunteer and we wish her the best in this next chapter. And in her honor, we will continue with the drive and intelligent planning LTG Lawrence demonstrated.

For example, here at the Signal Center of Excellence we are strengthening the defense of our networks and we are excited by the teamwork and excellent synergy between the different centers of excellence.

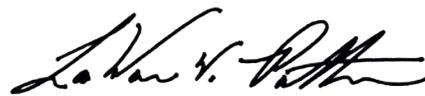
We have proposed creating three new military occupational specialties for cyber defense - one for non-commissioned officers and one for warrant officers and one for commissioned officers. And these Soldiers will not be neophytes. All must have significant network experience before being accepted into the various specialties.

Already, we have trained several cohort groups of warrants in our relatively new 255S course, which is called information protect.

Our Soldiers will learn about cyber forensics, protection of critical networks, penetration testing, vulnerability assessment, hacker techniques, voice over IP security and wireless security.

Thank you LTG Lawrence for setting such a solid foundation from which our Signal Regiment will continue to reach for the stars.

Pro Patria Vigilans!



[Join the Discussion](#)

<https://SIGKN.army.mil>



COMMAND

Chief of Signal
MG LaWarren V. Patterson

Regimental Chief Warrant Officer
CW5 Todd M. Boudreau

Regimental Command Sergeant Major
CSM Ronald S. Pflieger

EDITORIAL STAFF

Editor-in-Chief
Larry Edmond

Art Director/Graphic Designer
Billy Cheney

Photography
Billy Cheney, SPC Edwards Bates

By Order of the Secretary of the Army

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

Official:


JOYCE E. MORROW

Administrative Assistant to the
Secretary of the Army

Authorization 1409106

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

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

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

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 Center of Excellence and Fort Gordon, Signal Towers (Building 29808), Room 713, Fort Gordon, Ga. 30905-5301. Telephone DSN 780-7204 or commercial (706) 791-7204. Fax number (706) 791-3917.

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

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

ARMY COMMUNICATOR

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

PB 11-13-04
Winter 2013
Vol. 38 No. 4

Voice of the Signal Regiment

Table of Contents

Features

- | | |
|---|---|
| <p>5 Strategic Landpower for the Company Commander
GEN Robert W. Cone
CPT Jon D. Mohundro</p> <p>10 Network Operations in The Cloud
David Verret
Tim Wall</p> <p>18 Network Operations Initiatives
Derrick Smith
Terry Dawkins</p> <p>21 1st Cyber Network Defense Specialists Graduate
Wilson A. Rivera</p> <p>22 Tactical Public Key Infrastructure Concept of Operations Published
Michael Jones
Jimmy Kilgore</p> | <p>28 Active Shooter Approach Offers Operations Protection
 LTC Phillip G. Burns</p> <p>34 Simplifying NETOPS through Holistic Approach
Amy Walker</p> <p>37 NETOPS Common Services Dictionary
Robert Dillow
Sam Edelman</p> <p>40 Think Write Publish
 Joe Byerly</p> <p>44 Letter to the Editor</p> |
|---|---|

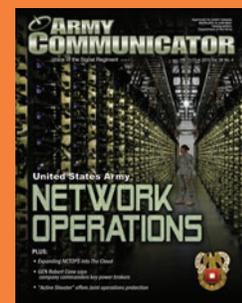
45 Center for Army Lessons Learned

Turn to page 45 to connect to the Army's CALL Center to check out the latest publications offering up-to-date lessons learned from Soldiers and leaders actually engaged in operations.

Join the Discussion

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

Cover: *This edition of the Army Communicator offers a framework outlining what falls within the network of computer and telecommunications systems and equipment necessary for the Army to operate effectively. This issue also addresses some of the current operational environment challenges that make it necessary to adapt at a pace that matches astonishing technological advancements.*



Cover design by Billy Cheney

Network Operations: A Signal Regiment core competency

Signaleers,

In this NetOps edition of the Army Communicator, I'd like to share my perspective that NetOps is a Signal Regimental "Core Competency," which means that Army NetOps is a function that should be trained exclusively at Fort Gordon; performed by Signal leaders and Soldiers at all echelons and is a function that no other TRADOC school or Center of Excellence has as a core competency.

NetOps is the Signal support component to Army operations that operates, manages, protects and defends networks from post/camp/station to deployed tactical networks. NetOps enables the Signal staff at all levels to execute commanders' priorities throughout the LandWarNet and allows commanders to utilize Mission Command Systems to effectively communicate, collaborate, share, manage, and disseminate information.

During the past 12 years of deployments in

support of OEF/OIF, our Signal Soldiers have fallen in on an established fixed network and infrastructure with a host of Field Service Representatives who have largely performed NetOps functions that in the past were performed by Signal Soldiers. This has created a generation of Signal leaders who lack the experience and knowledge to properly plan, engineer, install, operate, defend, govern, resource and conduct NetOps in today's dynamic environment. This problem has surfaced numerous times during re-deployment After Action Reviews and during "lessons learned" sessions with our Signal Soldiers and leaders.

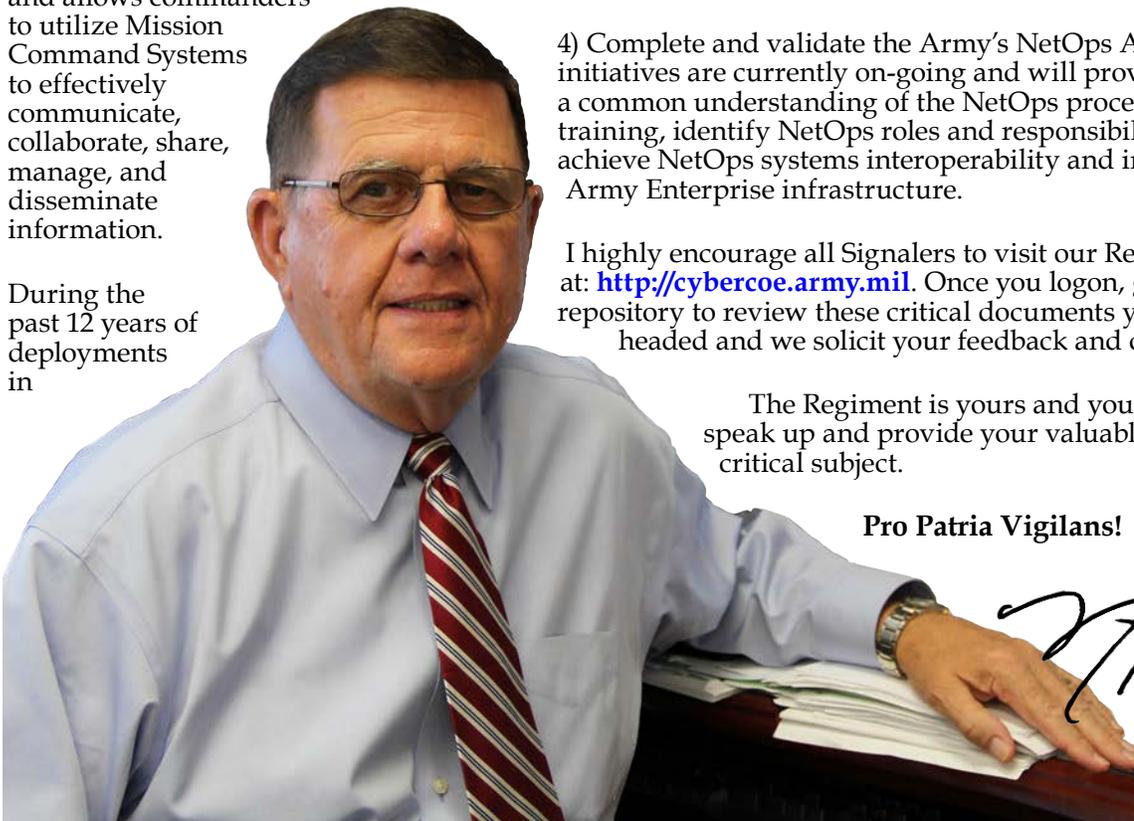
To help solve this problem the Signal Center of Excellence is facilitating several key initiatives:

- 1) Update and publish our "keystone" Doctrinal Field Manual FM 6-02, Army Signal Operations.
- 2) Update and publish ATP 6-02.71, Techniques for LandWarNet Operations.
- 3) Lead a CIO/G6 initiative to develop and publish an authoritative Army Enterprise NetOps Concept of Operations.
- 4) Complete and validate the Army's NetOps Architecture. These initiatives are currently on-going and will provide the framework for a common understanding of the NetOps process, improve NetOps training, identify NetOps roles and responsibilities by echelon and achieve NetOps systems interoperability and integration across the Army Enterprise infrastructure.

I highly encourage all Signalers to visit our Regimental web portal at: <http://cybercoe.army.mil>. Once you logon, go to the Doctrine repository to review these critical documents you'll see where we're headed and we solicit your feedback and comments.

The Regiment is yours and you are its future, so please speak up and provide your valuable insights on this critical subject.

Pro Patria Vigilans!



Warrant Officer cohort positioned to support NETOPS elements

Signaleers,

This edition of the Army Communicator focuses heavily upon Network Operations. Several years ago the Signal warrant officer cohort was transformed around the NetOps construct. A single warrant officer MOS was established to focus solely on each of the three elements of NetOps; content management, network management, and network defense. See the 2011 Vol 36 No 1 edition of the Army Communicator for more details. We are well on our way to shape the Signal warrant officer cohort under this construct and believe that it not only better focuses each of the MOS but also provides a singular POC for the S/G6 for each of the three elements of NetOps.

A continuing effort here at the Signal CoE is to work to influence industry to reduce the complexity of the equipment manufactured for the Army. While I don't want to reduce this pressure, we need to make sure we are comparing apples with apples. Let's maintain the pressure by comparing terminal devices (for example) with terminal devices; a tablet loaded with easy to use applications is a fair comparison of some of the complex Battle Command terminal devices.

However, just as one cellular company pictures a single user backed by a myriad of employees needed to present and maintain the best

user experience, NetOps is complex and it will likely remain so for the foreseeable future. This complexity takes a lot of work and keeps you all busy and on your toes.

As the Army maneuvers through a time of fiscal uncertainties in an environment of global power shifts, we need you to remain engaged. It is easy to be busy; busyness seems to be a badge of honor. But there is a distinct difference in busyness and productivity; these are not mutually inclusive terms. Busy \neq Productive; and conversely, Productive \neq Busy.

While many concede the first, the second is not so intuitive. Maybe this is why human beings are about the only living beings that when lost or confused tend to run faster.

Should the future fiscal reality result in less change to our infrastructure, I challenge our Signal warrant officers to refuse to give in to

the misconception that we must do "more with less." In fact, let us not even strive to do better with less, but rather better with what we have. Help us to work through the complex systems-of-systems we have fielding thus far, better understand and leverage the integration and synergy of NetOps, and get all we can get from what we have.

Stay engaged, be productive, and again, thank you for your dedication and service in being ever Watchful for Our Country.

Pro Patria Vigilans!



Evolving cyberspace defense role requires concerted efforts

Signaleers,

The Signal Regiment will need to recruit and train nearly 1,500 enlisted Soldiers in cyber defense over the next five years and we are going to need your help to make it happen.

We graduated the first class of the new 25D Cyber Network Defenders here at Fort Gordon on 27 November 2013. These men and women will join the 255S warrant officers on teams that defend our network, in addition to other key cyberspace defense positions. The recent graduates will lead the Army's effort to fill 1,460 Cyber Network Defenders' positions in the active, guard and reserve components of the Army.

Our 25D Soldiers will be the vanguard in cyberspace to ensure our Soldiers and leaders can rely on our communications network.

It is a highly selective process to be accepted into the 25D program and the Signal Center of Excellence needs about six applicants to find one Soldier who qualifies for acceptance into the 25D class. We will need a large number of applicants to fill those 1,460 positions over the next five years. That's why we need your help.

Of those 1,460 positions, the active duty Army will have 714 slots for 25D Soldiers on units' Table of Distribution and Allowances and Modification Table of Organization and Equipment books by fiscal year 2015. Until we train enough 25D Soldiers, a 25B can hold the MTOE slot, for now.

If you have Soldiers with unquestionable character with solid IT and IA experience, talk to them about the 25D MOS. And not just Signal Soldiers. The 25D MOS is open to Soldiers in any MOS. They receive valuable training, such as principles of cyber forensics and hacker techniques, penetration testing, vulnerability assessment, communications security and voice over IP security and wireless security.

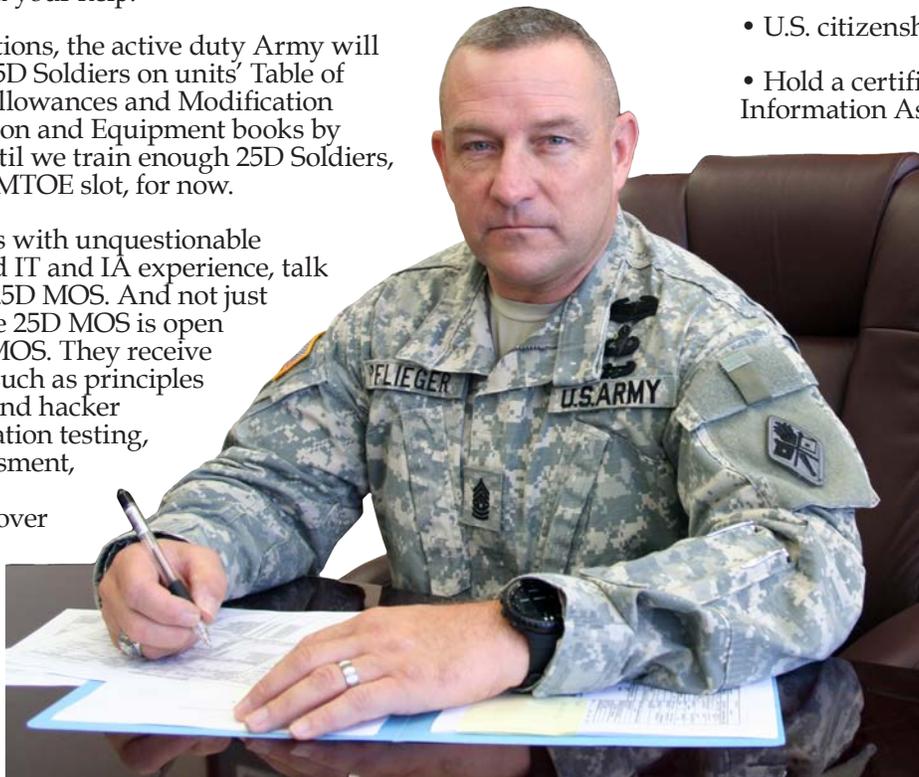
To apply, candidates will need a letter of

recommendation from a Lieutenant Colonel or above in their chain of command and the following prerequisites:

- A GT and ST score of 105 or better on the ASVAB.
- Normal color vision.
- A SSG or above with a TS-SCI clearance, MOS immaterial, with at least four years of IA/IT experience.
- At least eight years time in service, but no more than 17 years.
- A graduate of the Advanced Leader Course.
- U.S. citizenship.
- Hold a certification under Information Assurance Training Level II or Information Assurance Management Level I.
- Pass the 25D In-Service Screening Test, which is an accession and personality exam.

To learn more about the 25D MOS and find an application packet, visit www.us.army.mil/suite/page/838.

.Pro Patria Vigilans!





STRATEGIC LANDPOWER FOR THE COMPANY COMMANDER

*By GEN Robert W. Cone
and CPT Jon D. Mohundro*

In Iraq and Afghanistan, a generation of officers grew up solving strategic dilemmas at the company and platoon levels. Well-versed in the requirements and responsibilities of an Army at war, this generation must guide the Army into an ever-evolving and uncertain future. In order to navigate through the complexities in front of us, the Army needs capable, adaptable leaders now more than ever who champion the Army's strategic purpose and goals. With that, one of the most important discussions over the next few years will be how company commanders understand and implement the Army's central role in strategic landpower.

Over the last two years, the Army has put a lot of great people to work examining every facet of our training, doctrine, and warfighting capability. We did not do this to examine where we stand today. Rather, all of this effort was aimed at figuring out two things: what kind of Army we will need to meet future challenges, and what we have to do to build that Army even as we continue fighting in

Afghanistan and remain engaged throughout the world. Much of what we concluded is available in a single brief document – TRADOC Pamphlet 525-3-0, The U.S. Army Capstone Concept, <http://www.tradoc.army.mil/tpubs/pams/tp525-3-0.pdf>. If you have not read it yet – please do so.

We won't summarize an already brief document in this article. Instead, we will discuss how the newest and most vital ideas relate to the execution level – the company. While things have been written about strategic maneuver, nothing has been written about its application at the tactical level. Although some ideas may be new, much of what must be done remains the same – training, standards, and understanding the human environment. This is a result of the unchanging character of the Army's basic strategic problem and mission. As in prior eras, as part of the joint force, our Army must retain its ability to protect U.S. national interests, execute any mission assigned to us, and win on any battlefield around the world.

Given our national strategy, we are

(Continued on page 6)

required to field an Army capable of waging war decisively. Fielding a ready and responsive force with sufficient depth and resilience to wage sustained land combat is central to our mission, and that force must be able to conduct both combined arms maneuver and wide area security. A ready, robust, responsive force deters adversaries, reassures allies, and, when necessary, compels our enemies to change their behavior. Maintaining such a force requires high levels of adaptability throughout each echelon of the Army. Only Soldiers with tactical skill and operational flexibility can effectively respond to changing tactical situations in support of our nation's strategic goals and interests.

This is where the company commanders fit into the concept of strategic landpower. Much like company grade officers did in Iraq and Afghanistan, the company commander of the future must be mentally agile enough to thrive within the parameters of mission command.

Developing leaders who can do so, while providing clear task and purpose to their subordinates, will be critical to the success of any mission across the range of military operations. Effective Army commanders, including

“It is the responsibility of senior Army leaders to set the conditions to make you, and our Army, successful. Your senior leaders appreciate what you do every day.”



- GEN Robert W. Cone
Commanding General
U. S. Army Training and Doctrine Command

those at the company level, do not use fiscal constraints as an excuse for failing to develop the best possible mix of training, equipment, and regional expertise they can within their formations. Rather, they motivate their people and guide their units in a way that makes optimal use of available resources to create adaptive, effective forces.

Our Army has three primary and interconnected roles: prevent conflict, shape the international environment and win the nation's wars. The company commander has important responsibilities in each of these.

Prevent Conflict

It is prudent here to define what a conflict is. Since the term gets thrown around a lot and attached to a lot of different situations, it is easy to misunderstand the doctrinal meaning. Conflict is an armed struggle or clash

between organized groups within a nation or between nations in order to achieve limited political or military objectives.

Irregular forces frequently make up the majority of enemy combatants we face now, and may continue to do so in the future. Conflict is often protracted, geographically confined, and constrained in the level of violence. Each one also holds the potential to escalate into major combat operations.

Many of the contingencies to which the United States responded militarily in the past 50 years have been appropriately defined as “conflicts.” The same can reasonably be expected in the future, but with the addition of cyberspace.

As was true during the Cold War, many of our greatest successes in the future will not occur on the battlefield; rather, maintaining peace may be our greatest achievement. This will be no

easy task, as global tensions and instability increase in ungoverned or weakly-governed spaces around the world. History has taught us that without a capable, highly trained land force, the United States has little influence in many of those spaces. That land force, our Army, must remain the best equipped, best trained and most combat ready force in the world if it is to have the strategic effect we seek. That readiness is built from the bottom up.

This is the first critical point where company commanders must help shape the future. As owners of the training schedule, commanders have the critical role in developing team, squad, and platoon skills. Commanders ensure that broadening training like language, geographical and cultural familiarization is done effectively, in a rigorous manner.

Soldiers from the generation that fought in Iraq and Afghanistan will not be satisfied with training focused on artificial scenarios and made-up adversaries, so their commanders need to be innovative about preparing well-coordinated, realistic training. Subordinates must be challenged, and they have to feel their challenges have a direct linkage to future operations. In order not to lose 12 years of combat-proven leader development, company grade officers must find a balance between building an Army prepared for the range of military operations and succumbing to pressure to “get back to the way it used to be.”

Unfortunately, possession of such a trained and ready force is useless if it cannot affect regions where trouble is brewing. As units reposition from overseas bases and return to the United States, it becomes more crucial than ever for the Army to adopt an expeditionary mindset and improve its expeditionary capability. To do so the Army is aligning units to specific geographical regions and arranging them into scalable and tailored expeditionary force packages that meet the needs of the Joint Force Commander

across the range of military operations. In short, our Army will be better postured to generate strategic influence anywhere in the world, and as part of the joint force, deter aggression.

In this construct, company commanders must conduct operational environment training specific to their region. Becoming familiar with the people, cultures, and languages of the region in which one’s unit will operate is critical to the success of a CONUS based Army. Conventional-force companies learned much over the past 12 years as they executed missions historically reserved for Special Forces.

War is fundamentally a human endeavor, and understanding the people involved is critically important. Company Commanders cannot now ignore the hard-won lessons of their predecessors by ignoring one of the Special Forces’ key tasks of understanding the operational environment. Those who meet this intent and enforce standards during this training will ensure we pay those lessons forward to the next generation.

Shape the Operational Environment

During peacetime, the Army is continuously engaged in shaping the global environment to promote stability and partner nation capabilities. We do this for several reasons, the most important of which is maintaining peace in pursuance of American national security interests. Where conflict has already broken out, engagement helps keep it contained and may even lead to a peaceful resolution. By helping to build partner capacity and trust, forward engaged Army units greatly add to regional and global stability. Moreover, by building strong relationships of mutual trust we facilitate access and set the conditions for success in any future combined operation in a particular region or country.

(Continued on page 8)

(Continued from page 7)

But what are shaping operations, and how are they executed at the company level? Shaping operations are defined as those operations, occurring at any echelon, that create or preserve conditions for the success of the decisive operation. Thus, engagement by regionally aligned forces positively shapes the environment in which the Army operates throughout the range of military operations.

This aligns with the notion of the “strategic corporal,” which recognizes that in the information age the actions of individuals and small groups can have widespread impact well beyond what was intended at the time. Every action has a reaction, and it is necessary for junior officers to be aware of the role their Soldiers and unit play in the overall strategic goals of our nation.

As part of regionally aligned shaping operations, the Army will employ a careful mix of rotational and forward-deployed forces, develop relationships with foreign militaries, and conduct recurring training exercises with foreign partners to demonstrate the nation’s enduring commitment to allies and friends. Where we share mutually beneficial interests with an ally, the Army enhances that partner’s self-defense capacity and improves its ability to serve as a capable member of a

future military coalition. More capable allies generate a stabilizing influence in their region, and tend to reduce the need for American military interventions over time.

Shaping operations do not end with planned training engagements by forward deployed units. Other actions the units or even small groups of individual Soldiers take can have a shaping effect. Those actions will run the gamut from brigade or division - sized assistance after a natural disaster to a single act of kindness to a foreign student in an Army school who later rises to high levels in his nation’s armed forces.

Regardless of the specific activities that have a shaping effect we conduct, all should convey to our intended audiences the clear message that while we are committed to peace, our nation protects its friends and defends its interests. Instilling this understanding among our Soldiers and junior NCOs is one of the vital roles the company grade officer plays in the execution of strategic landpower.

But there is a caveat. What may be the standard for us is not necessarily useful or welcomed with our host nation partners. So, shaping also entails tailoring our delivery of security assistance to our counterparts in ways appropriate for their culture and military capabilities. Company commanders can gain great success here by

applying key interpersonal skills to know, understand, and be humble when dealing with officers, NCOs, and Soldiers from other armies. Win the Nation’s Wars

Despite our best efforts to shape a stable global environment and prevent conflict, violence is likely to remain endemic to the human condition. As been said, “Only the dead have seen the end of war.” While we do everything possible to prevent the outbreak of war, we must ensure there never will be a day when the U.S. Army is not ready to fight and win wars in defense of our nation.

What is a war?

Historically, war has been defined as a conflict carried out by force of arms, either between nations or between parties within a nation. However, as we consider hostile acts in cyberspace, the definition of war and acts of war will continue to evolve.

For example, large-scale cyber attacks against government operations or critical infrastructure – such as in the 2008 Russian-Georgian conflict – can reasonably be considered acts of war.

Leveraging the technological savvy of today’s Soldiers requires leaders with an engaged interest in their development. This will require junior leaders from the same generation who are as adept at leader development as they are technologically competent.

To defend our Nation, the Army must maintain the capacity to conduct strategically decisive land operations anywhere in the world. Though we will always conduct such operations as part of a joint force, we also acknowledge that war is a clash of wills that requires the ethical application of violence to compel change in human behavior. Here, company commanders make a dramatic contribution to the application of strategic landpower by being tactically and technically proficient in the execution of combined arms maneuver and wide-area security. Without successful tactical execution, the best strategic concepts are doomed to failure.

The U.S. Army Capstone Concept lays out the details of what capabilities the Army must sustain, as well as provides some guidance on how the force may be employed in the future. But it all boils down to one crucial point; an Army that cannot win on the battlefield is of little worth to the security of the nation. As everyone is aware, we are facing austere times ahead. This fiscal reality cannot be an excuse for not doing our duty or losing sight of our purpose. In the final analysis this country will one day - maybe soon - ask us to deploy to some distant land, close with and destroy an enemy, and then build a secure and lasting peace. Our

Army is uniquely qualified to ensure the training necessary to make those things happen, thanks to the strength of our NCO Corps. Commanders must leverage the experience of their senior NCOs and find creative ways to properly train the fundamentals, despite resource constraints. We've successfully done it before in our Army, and we are counting on our young leaders to do it again.

Conclusion

It was often platoon and company leadership who took the lead solving strategic issues in Iraq and Afghanistan. It will continue to be platoon and company leaders who keep the Army

the well-trained and globally-responsive force our Nation needs to deter our adversaries, protect our friends, and defeat our enemies in the 21st century.

The U.S. Army must have company commanders who understand Strategic Landpower and their role in it. Seek out opportunities to ingrain your training events within the framework of Strategic Landpower. Write articles in your branch's professional journal discussing the impacts of Strategic Landpower for your specialty. You can find the Strategic Landpower white paper on the TRADOC internet homepage at http://www.arcic.army.mil/app_Documents/Strategic-Landpower-White-Paper-06MAY2013.pdf, and on company commander discussion forums. This white paper is the primary reference for Strategic Landpower concepts and the one jointly approved by the Army Chief of Staff, the Marine Corps Commandant, and the Commander of U.S. Special Operations Command.

It is the responsibility of senior Army leaders to set the conditions to make you, and our Army, successful. Your senior leaders appreciate what you do every day. These will be challenging, but exciting times, and I thank you for your service and sacrifice as we move towards making the Army of 2020 and beyond the best in the world.

Seek out opportunities to ingrain your training events within the framework of Strategic Landpower. Write articles in your branch's professional journal...

Network Operations in The Cloud

By David Verret and Tim Wall

This article gives an update on the U. S. Army Training and Doctrine Command Capability Manger for Global Network Enterprise's cloud computing and related capabilities that will affect all Department of Defense elements.

The primary driver for the cloud computing initiative is to gain efficiencies by maximizing the use of computing resources by numerous users. This is accomplished by leveraging shared infrastructure and taking advantage of economies of scale that make cloud computing such an attractive business model for many organizations.

The DoD and its agencies are at various stages of maturity in planning and implementation of cloud technologies. The cloud initiative began formally in 2011 with the federal government mandate for the "Cloud First" computing strategy; the Federal Data Center Consolidation Initiative, Army Data Center Consolidation Plan, and other directives soon followed. In response, the U.S. Army has formed the Army's Cloud Synchronization Working Group.

This group meets regularly to carry out the essential tasks of analyzing, planning, and implementing enterprise cloud computing to ensure proper integration into the DoD Joint Information Environment and also to the Intelligence Community Information Technology Enterprise.

Background

In response to the Army Chief Information Office / G6's LandWarNet 2020 and Beyond Enterprise Architecture, the Assistant Secretary of the Army for Acquisitions Logistics

and Technology identified six computing environments:

- The Data Center/Cloud/Generating Force CE
- Command Post CE
- Mounted CE
- Real-Time/Safety/Critical/Embedded CE
- Mobile Hand-Held CE
- Sensor CE

ASA (ALT) and Program Executive Office, Enterprise Information Systems are the leads for the Data Center/Cloud/Generating Force with TCM GNE and TCM Mission Command leading the DC/C/GF CE Requirements Sub-work Group under the guidance of the Mission Command Requirements Governance Team. Other sub-working groups under Cloud Synchronization Work Group are involved in the planning of technical, financial, and management areas.

The first Army Cloud Summit Conference was held at Fort Belvoir, Va. in June 2013. Each of the sub-working groups discussed the important issues and concerns of key stakeholders and made plans for the future integration of enterprise information service capabilities delivered from data centers to the Generating and Operating Forces. The U.S. Army CIO/G6 is currently working on the Army Cloud 2020 Vision and Conceptual Architecture while TCM GNE and TCM Mission Command are working on the Cloud Concept of Operations document. PEO EIS is developing the Army's Data Center Cloud Computing Environment Architecture to integrate into the future Joint Information Environment Core Data Centers (see Figure 1).

Cloud Computing

It should be noted that there is no universally agreed upon definition of a

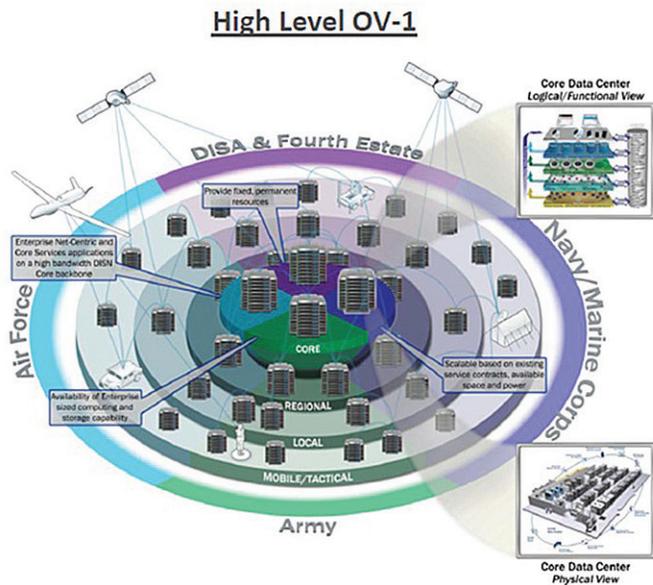


Figure 1 Joint Information Environment Core Data Centers

cloud; however, there is agreement on the characteristics or attributes of a cloud. Specifically, the National Institute of Standards and Technology issued a special publication, Cloud Computing Reference Architecture (SP800-145), which defined many of the characteristics and attributes of a cloud computing model and the Army endeavored to closely follow the NIST Reference Architecture. According to NIST, cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model is composed of five essential characteristics, three service models, and four deployment models. A prime reason for many organizations to use cloud computing is never having to build or maintain the organization's own data center and not having to pay for upfront infrastructure or the associated costs like buildings, employees, electricity, etc. With cloud based hosting, the applications' owner

only pays for computing capacity consumed. Even the DoD will outsource for cloud computing when commercial cloud service providers are able to comply with federal guidelines and security regulations.

Initially, Defense Information Systems Agency will manage eight Joint Information Environment Core Data Centers which are geographically and strategically located in Defense Enterprise Computing Centers.

New Information Technology services for Programs of Record and non-PORs are scheduled to be hosted in DoD data centers as early as FY 14. The DoD CIO has directed that all enterprise applications be moved to CDCs by FY18.

Deployable data centers are planned for the tactical computing environments for certain phases of operations and, as part of the JIE concept, are known as Installation Processing Nodes – Tactical.

However, there still remains much planning and work to be done to upgrade the network capacity and required infrastructures to support cloud computing capabilities.

Organizations will have to set-up and coordinate Service Level Agreements with the cloud service provider to ensure Quality of Service requirements are established.

Basics

Conceptualizing the boundaries of cloud computing components requires the notion that there are few clear borders between some of the service models. The three most typical cloud service models shown in the diagram depicted in Figure 2 are:

- Infrastructure as a Service
- Platform as a Service
- Software as a Service

Let's consider what these three service models mean in context of the cloud for a cloud subscriber/Soldier.

(Continued on page 12)

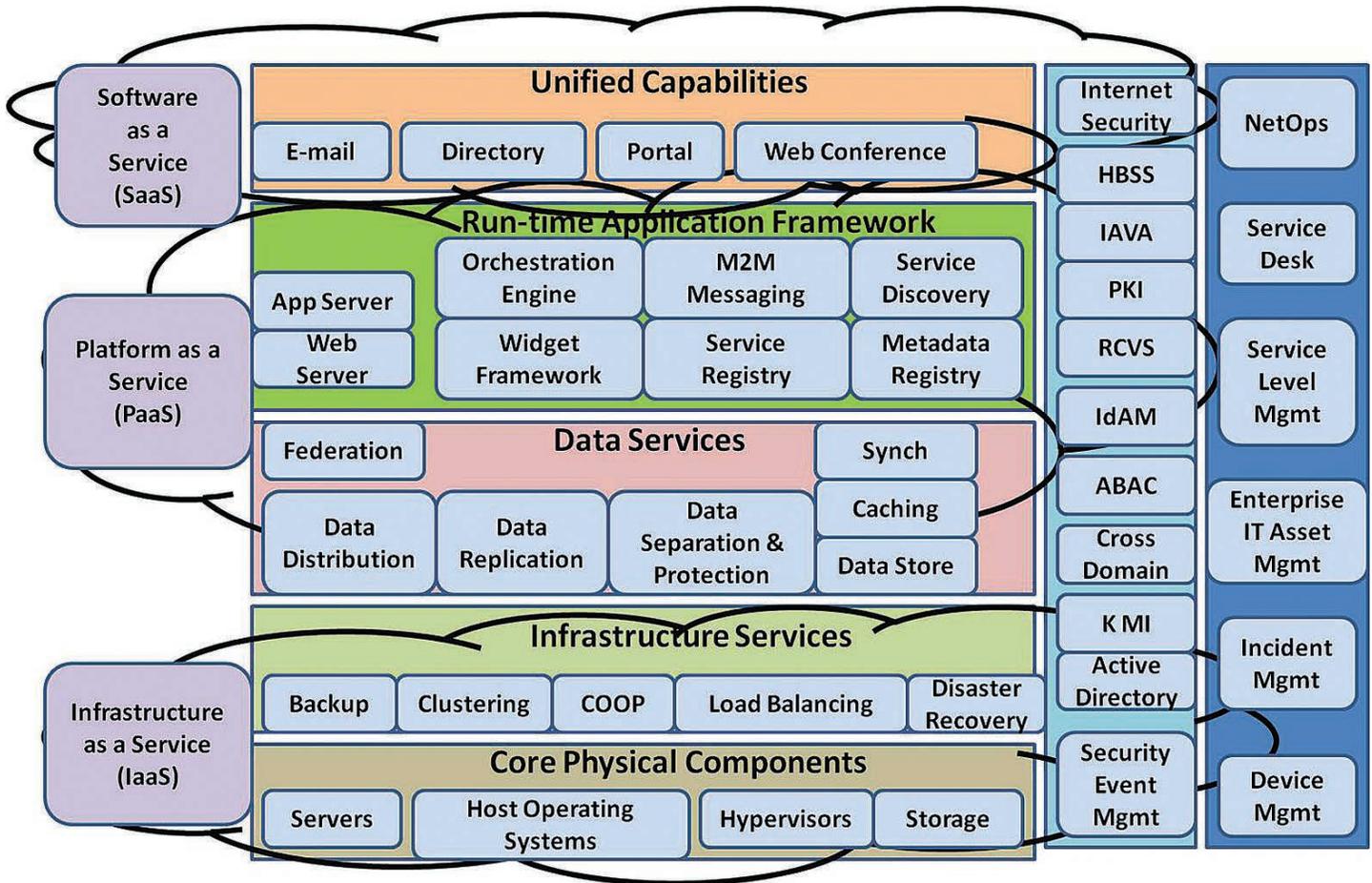


Figure 2 Typical Cloud Service Models

(Continued from page 11)

In terms of infrastructure or IaaS, it means that the Soldier doesn't necessarily need an expensive laptop or personal computer. A less expensive and simpler device e.g. thin client/zero clients can replace it.

The benefit of thin client/zero client utilization is that it doesn't need continual technology or software upgrades or security updates. If the device is discovered missing or destroyed there is no data loss and improves information security because the critical data is stored and managed remotely.

A thin client/zero clients can be a very simple computer with only enough capability to communicate with the terminal services server. The terminal services server can be compared to the old mainframe computers that were accessed via "dumb terminals." All the computer processing is done remotely. The applications are run in virtual machines with many VMs running on a single physical machine in a data center. Replicating this approach across hundreds of applications means a much smaller number of physical servers are required in a data center.

Using modern cloud management software tools allows data center personnel to manage significantly more applications with significantly less "touch labor."

The complexity is reduced for the network technician and Help Desk functions in that instead of having to manage, update, and maintain hundreds of individual servers, PCs, and laptops, now the focus is on the terminal services server and the virtualized applications. The result is efficiencies gained in work-hours, cost, centrally managed security, and asset accountability.

The next service model,

Platform as a Service, is mainly used by computer and software developers to work on new computing capabilities. In traditional software development, the developers would need to either build certain utilities or other software tools necessary to support the application software or reuse existing tools.

These tools and utilities are commonly referred to as the “middleware” because they generally sit between the operating system and the mission specific applications. Common examples of this middleware could be a web server or database management software.

In cloud computing, the PaaS is the set of common utility services and tools pre-exist and are pre-integrated that allow the developers focus on development of the mission specific application code. This not only saves time for the developers, but also provides a set of common interoperable tools that have been configured to meet security requirements.

While these tools are used by the mission applications during execution, generally the end users are unaware of the operation of these middleware tools during their use of the application.

Only the most technical and experienced Signal Soldiers will have access to this service and will be able to easily set-up an application and configure customized

services at will. This means a Commander or organization will not have to buy servers, hire IT professionals, operate and maintain their own server rooms, pay for maintenance, pay for electric bills, or buy and maintain expensive security systems for their facilities. PaaS is often combined with the other service models but can be a separate service also.

The final service model is called Software as a Service. SaaS are complete applications that end users access and organizations pay for use of those applications. Organizations do not have to pay for the development, testing, deployment or maintenance of the application but typically pay by number of users for a set period of time.

Defense Enterprise Email provided to the Army by DISA for a fixed cost per year per user is an example of a SaaS application. The important principle of this service is that it is platform independent. This means that the software program will work on any type of end user device like a PC, tablet, phone, or even game consoles.

Whenever you open your web browser and have used commercial web hosted email or any other “App” you have used some form of SaaS. Google Search and Google Docs, are good examples of SaaS Apps. The U.S. Army has many Apps created for smart phones and other devices, too. There are Apps to calculate

physical fitness test scores, body fat, newsfeeds and other notifications; the list goes on and on. If interested in the Army Apps go to <http://www.army.mil/mobile/> and see what is available from the Army App Store.

Virtual Machines

Virtualization is what everyone thinks of when the topic of cloud computing is discussed. Virtual machines are a component of cloud computing. Cloud computing is far more than simply creating and using virtual servers because it includes many more cloud technologies, processes and delivery methods.

Virtual computing is the ability to separate the operating system and applications from dedicated hardware. Essentially, the operating system, commercial off the shelf tools and the mission application are packaged into a VM.

One or more VMs can be hosted on a single physical machine and the hypervisor, which resides between the VM and the physical machine, prevents one VM from interfering with operation of the other VMs. This mechanism for packaging the OS, tools, and application allows the transfer of the operating system, settings, and the applications to another set of servers and everything stays together and in working order.

(Continued on page 14)

In older or less capable systems, if you wanted to migrate your server, applications, and databases, it was a tedious and often painful process that took 24 hours or more to complete if everything was done right. This could be a very expensive task if you are paying a person by the hour; with virtual computing it might take minutes or hours depending on how much data is being migrated. Typically, the VM can be moved from one server to another using modern cloud management software, (in the same LAN) without even stopping execution of the application.

Clusters

One of the benefits of cloud computing is the process of clustering. A cluster is a group of interconnected servers in a data center that are running similar operating systems (and sometimes dissimilar ones) that have a database system such as MySQL (pronounced: my es Q el or my sequel). Nearly all the tasks that are done in web-applications require some type of data storage. MySQL is a data storage system that shares information with other clustered MySQL systems.

The point of this is that if one server fails or has reached maximum capacity then the user's access to the application and data is redirected to another server automatically.

This process is known as load balancing. In the old days if the server failed or was at capacity, the user was out of luck (no more computing or loss of all the data). In cloud computing this is not a concern if it is implemented correctly. Continuity of Operations and Disaster Recovery are also enabled by clustering.

Hosted Instances

Another term you will hear is called hosted instances. This means that your Warrant Officer 255A will be able to place an application in a future Army data center or one of the Defense Enterprise Computing Centers and use it as needed.

The use of hosted instances in data centers need special planning and consideration, one of those is network latency. Network latency is the delay induced by the network in transmitting data between two endpoints (e.g., between the data center where the application is hosted and end user computing device).

The amount of delay induced is determined by many factors, with the primary factor being the network bandwidth or capacity of each of the links that the data must be routed through to reach an endpoint (where the slowest link in the path being the driving factor).

Other factors include the traffic load on a shared network and, in the case of access via a wide area network, the geographical distance that the data must traverse. If the network path includes a satellite hop, this will contribute significantly to the latency.

Even robust terrestrial networks can have time-distance issues. In general, it is better to be closer to the data center for faster data throughput speeds.

Unfortunately, closer proximity may not be possible so the DoD has planned to use smaller locally available data centers called Installation Processing Nodes on base/post/camp/station which host edge servers. In a deployed environment there are plans to use small deployable data centers known as Installation Processing Nodes-Tactical or similar capability. By using hosted instances, a commander can leverage the benefits of cloud computing when it makes sense and only when it is feasible. Currently, TRADOC capability managers and other planners think that the servers/data centers/cloud will be (1) locally accessible, (2) operationally accessible and/or, (3) globally accessible. Look for more information in the future Expeditionary Forces Information Services Capability Production Document and the U.S. Army Cloud Enabled Network CONOPS.

Hosted Solutions/Services

Hosted IT solutions and services are provided by an enterprise cloud service provider like Amazon in the public domain or

the for the DoD community. The DISA Services Catalog offers a variety of enterprise services to the Components (Army, Navy, Air Force, Marines, and Coast Guard). The Joint community has embraced the concept of the JIE which will utilize CDCs. DECCs already host services such as the Multi-National Information System and others (See Figure 3).

One service that was implemented in 2012 is DEE. It is available from home station and planned to be available in deployed environments. The tactical version of DEE will likely be called Tactical Enterprise Email and will be hosted on forwardly deployed servers. DEE/TEE offers three fundamental capabilities: email, calendaring, and people discovery in the form of a global persona directory.

DEE and the DEPS are available now and other Common User Services will be offered. TCM GNE is currently writing a Capability Development Document for Enterprise Information Services for future programming of resources to support these solutions/ services for LandWarNet 2020.

Mission Assurance Services

Mission Assurance Services are those services that proactively maintain the confidentiality, availability, integrity and non-repudiation characteristics of information

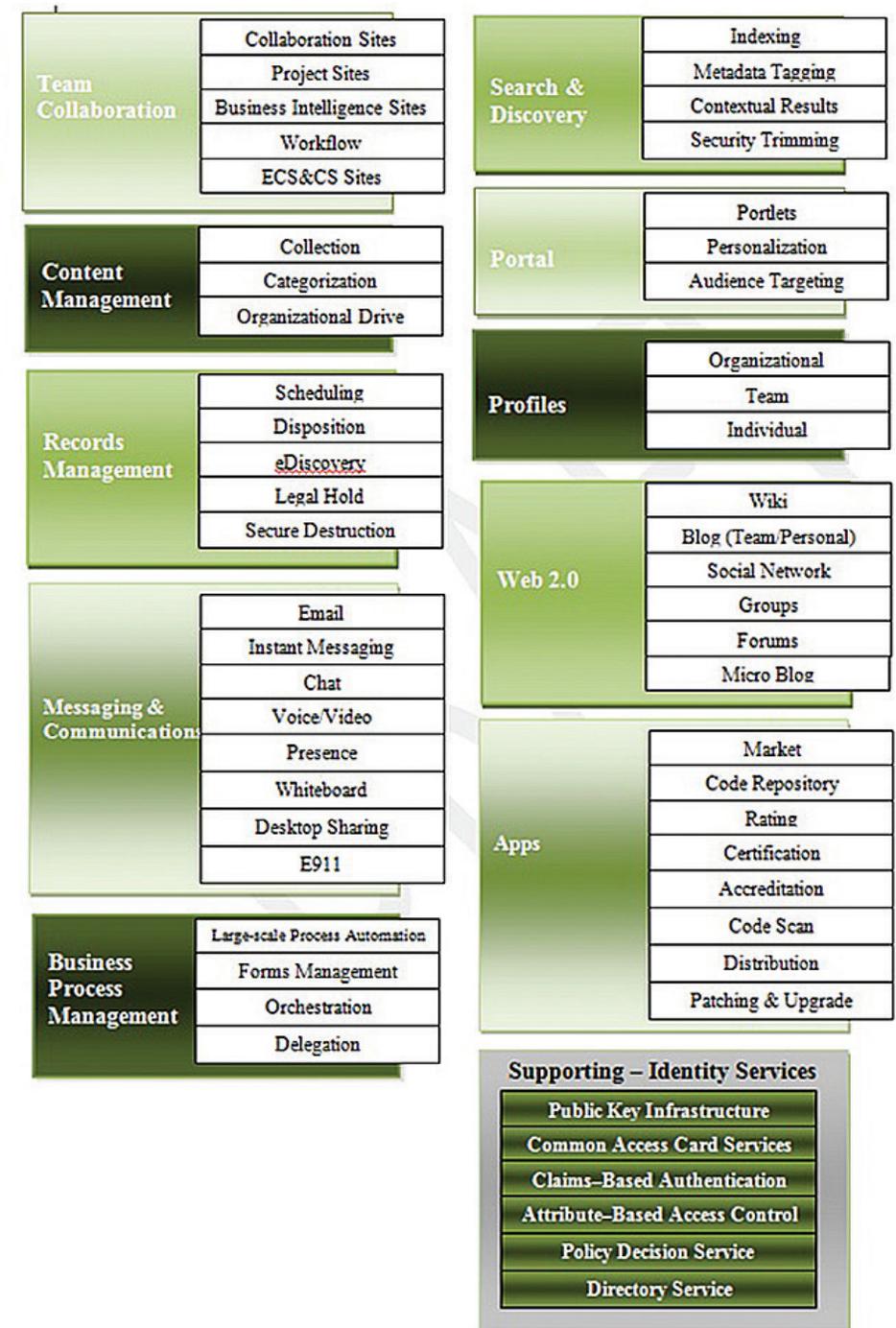


Figure 3 - List of Enterprise Services and Sub-Categories

stored in the cloud. In addition, the new architectures aim to improve efficiency by reducing duplication of operations, establishing joint protections and responsibilities by flattening the network. Security will

improve through dividing the network into manageable and securable zones; placement of sensors to inspect traffic; and centralize network operations functions. Through the use of

(Continued on page 16)

(Continued from page 15)

automated cloud management tools, applications and VMs can be continuously monitored for compliance with latest security requirements and configurations and, in many cases, automatically applying the latest security patches thereby significantly improving the overall cyber

security posture of Army mission applications. The most sensitive data and information will be only available to authorized users of the DoD private cloud computing environments.

Cloud Types

All clouds are not the same. There are public clouds like Amazon and Google that the

general public can use; private clouds that organizations have complete control and access; and there are hybrid clouds that combine both private and public. The DoD and the Army will use different types depending on the goal or mission. In a tactical environment and other DoD implementations, a private cloud(s) will be employed in a configuration that may be fixed or mobile, but, in either case will be secure and hardened. In other cases, such as the hosting of public information sites and social media on the World Wide Web, a public/commercial cloud will be used for functions like the Army recruiting websites.

Issues to Consider

Whether or not to operate and maintain one's organization's computing resources or to use a cloud provider is a critical decision that leaders shouldn't make without a thorough risk analysis. No system or process is perfect for every situation and adopting cloud computing is no different. Cloud computing may be the best solution to save costs for taxpayers. However, performance and security issues may be a serious problem for tactical users in deployed environments. Some issues are provided in Table 1 (on page 15 at left) as a basic guide.

Cloud Computing Benefits and Challenges		
Issues	Benefits	Challenges
Scalability	Quickly scales	Depends on Cloud Provider
Funding/Costs	Pay as you go Economy of scale	Custom requirements are expensive Building new data centers are expensive – high upfront costs DoD funding models usually assume long range planning for resource requirements
Security	Centrally managed, easier to audit, Cloud security experts manage versus "in-house" staff, Continuity of Operations	User trust issues, trusted security architecture, multi-tenant environment, impacts to enterprise, highly desired target for malicious hackers
Infrastructure	Cloud Provider (DISA or Army) provides Core Data Centers with infrastructure shared among many applications	Possible single point of failure
Availability	High availability, Automated failover within a data center	Network problems - Disconnections, Intermittent connections, Limited Bandwidth in Tactical Environment
Data Storage	Dynamic expansion, Shared storage resource pool	Possible unauthorized exposure in multi-tenant environments
Custom Applications	Excellent environment to develop, test, employ	Can be expensive and cost prohibited; vendor lock-in
Virtualization	Easy to do	Legacy systems may not be compatible - redesign may be necessary (expensive)
Migration of systems/data	Easy to do, Many automated tools available to support migration	Some clouds may not be compatible; costs involved, Regression testing usually required, Vendor Lock-in
Legal or Regulatory Issues	Can be compliant with Federal regulations; e.g. FEDRAMP, HIPPA, etc.	Trusted vendors, International laws, who owns the data? Where does data physically reside?
Performance	Fast computing in reliable and high capacity networks	Slow throughput / poor performance on some networks

Table 1 - Cloud computing benefits and challenges

Summary

Frankly speaking, what has been marketed as cloud computing is not new; one can trace the capability as far back as the 1950s and 60s when mainframes were a shared computing resource executing many applications. Back then it was called time-sharing; although the capabilities have progressed technologically and it is now available to everyone. Cloud users/customers are essentially buying services hosted on remote servers and measured by time and storage space that is consumed.

The main driver for the government and its agencies to use cloud service providers is an attempt at cost savings with added benefits of ubiquitous network access by multiple types of end-user devices. The DoD and the Army are rapidly moving towards using consolidated computing resources to gain efficiencies from economy of scale and from sharing computing resources among many applications vice resources dedicated to a single application.

From a business perspective, it appears that this will reduce costs in the long-term by changing the economics from spending on capital expenditures upfront to ongoing operational expenditures. Meanwhile, the

security and the process of managing data and the systems that support enterprise cloud computing are being considered very carefully especially for tactical users.

This is necessary before full implementation in the deployed environment. Rest assured, TCM GNE and others are working diligently towards analyzing the requirements from both the Generating and Operating Forces perspectives.

David Verret retired from the U.S. Army after 23 years of service and has provided contractor support to TCM GNE since 2009. He has earned Bachelor of Science and Master's Degrees and is currently pursuing his doctoral degree in information science.

Tim Wall is a principal engineer with the MITRE Corporation. He is currently supporting the Army PEO EIS CIO in the architecture, design, and implementation of the Army's Common Operating Environment Data Center Cloud Computing Environment.

Editor's Note--The opinions expressed in this article are those of the authors and do not constitute an official position of any agency or organization.

ACRONYM QuickScan

ASA (ALT) - Assistant Secretary of the Army for Acquisitions Logistics & Technology
CE - Computing Environment
CDC - Core Data Center
CIO - Chief Information Officer
CPD - Capability Production Document
DC/C/GF - Data Center/Cloud/Generating Force
DECC - Defense Enterprise Computing Centers
DEE - Defense Enterprise Email
DISA - Defense Information Systems Agency

DoD - Department of Defense
EIE - Enterprise Information Environment
EFIS - Expeditionary Information Services
GIG - Global Information Grid
IaaS - Infrastructure as a Service
IC ITE - Intelligence Community Information Technology Enterprise
IT - Information Technology
JIE - Joint Information Environment
LWN - LandWarNet
NIST - National Institute of

Science and Technology
OS - Operating System
PaaS - Platform as a Service
PEO EIS - Program Executive Office Enterprise Information Systems
PC - Personal Computer
POR - Program of record
SaaS - Software as a Service
TCM GNE - TRADOC Capability Manager for Global Network Enterprise
TEE - Tactical Enterprise Email
TRADOC - U. S. Army Training and Doctrine Command
VM - Virtual Machine

NETWORK OPERATIONS INITIATIVES

By Terry Dawkins and Derrick Smith

U.S. Army Training and Doctrine Command Capability Manager for Global Network Enterprise leaders are engaged with many Regimental partners to develop both an authoritative NetOps Concept of Operations and a NetOps Reference Architecture in a rapidly changing environment.

NETOPS between the Enterprise and the deployed environment is a key element in the integration of the Army's Network 2020 into the Joint Information Environment.

According to Joint Publication 6-0 Joint Communications System, NetOps is defined as "activities conducted to operate and defend the Department of Defense Information Network" formerly known as the Global Information Grid. Subsequently, within the Army those same activities enable operational, organizational, and technical capabilities for operating and defending the LandWarNet, the Army's contribution to DoDIN.

The purpose of the "U.S. Army Network Operations 2020 and Beyond Concept of Operations" is to establish a single authoritative concept on how the Army will operate, maintain, secure and defend on the road to Network 2020 within the JIE (See Figure 1). This concept serves as a basis for future NetOps capability documents and a guide for the transition of NETOPS in support of Directive 2013-02 (Network 2020 and Beyond: The Way Ahead). The CONOPS will also assist in describing the current NetOps environment and some of the key operational challenges faced by our Regiment.

Defining Army NetOps processes within a Joint construct will assist in documenting and standardizing NetOps through all echelons and Doctrine, Organization, Training, Materiel, Leadership, Personnel, Facility-Policy domains. Specific roles and responsibilities will be outlined for the various organizations that are expected to participate in the execution of NetOps

throughout the Army.

The CONOPS will also include annexes for a more in-depth explanation of NetOps in the Warfighter Information Network-Tactical and the Integrated Tactical Network Environment. Practical functionality of NetOps will be illustrated utilizing use case operational scenarios (vignettes) that capture common and abstract situations which demonstrate how NetOps processes are applied for operating and defending the Army's portion of the DODIN through joint operational phases 0-5.

Cyberspace is an evolving concept for an emerging warfighting domain. In order to properly operate and defend the LandWarNet, there must be a clear distinctive understanding of the difference between Cyberspace Operations and Network Operations. Within this CONOPS, cyberspace is defined as "the hundreds of thousands of interconnected computers, servers, routers, switches, and fiber-optic cables that allow our critical infrastructures to operate." The CONOPS will provide an overview of Army Cyber Command's role in Defensive Cyber Operations and intentionally exclude their role and responsibilities in Offensive Cyberspace Operations. Doctrinally, OCO is not a part of the Army NetOps construct.

This CONOPS will apply to active Army, Army National Guard / Army National Guard of the United States, and the United States Army Reserve. The proponent of the CONOPS is the United States Army Training and Doctrine Command. The leads overseeing preparation of the document are Headquarters Department of the Army Chief Information Officer / G-6 and United States Army Signal Center of Excellence. This CONOPS covers NetOps from the Enterprise to the deployed environment and any organizational network that follows Army Regulation 25-1, Army Information Technology. This CONOPS was approved for worldwide staffing by the CIO/G6 and TRADOC in February 2014.

Even before BG Albert J. Myer was a

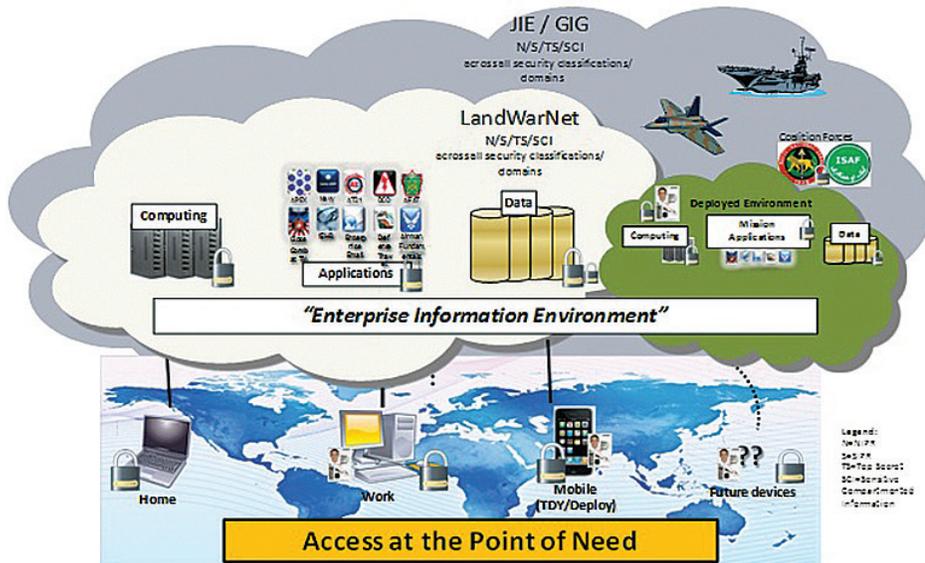


Figure 1

major, there was a need for communications in the U.S. Army. In today's Army with the emphasis on Information Technology, it is indispensable. According to Joint Publication 6-0 Joint Communications System, "Network Operations are activities conducted to operate and defend the Department of Defense information networks." Field Manual 6-02 Signal Support To Operations, Final Draft 14 Aug 13, states "Effective NetOps is the availability of service, which facilitates network enabled operations."

The question that comes to mind is this: how does an organization as complex as the U.S. Army Signal Regiment ensure the availability of service? Believe it or not, it should start with the Army NetOps Architecture. Never heard of it, right? That is about to change.

Prior to the ANA the Army did not have an integrated NetOps Reference Architecture.

According to the Department of Defense, a "Reference Architecture is an authoritative source of information about a specific subject area that guides and constrains the instantiations of multiple architectures and solutions." In other words, the ANA is a source you can reference when designing, building, configuring, securing and operating your networks. Using the ANA gives you a certain degree of confidence that you have a validated basis for your network.

The initial version, called the ANA (Operational), used the Infrastructure Technology Information Library as its foundation with the DoD Information Enterprise Architecture and Network Enterprise Technology Command's LandWarNet NetOps Architecture as references. It was completed in September 2012. The ANA Version 2.0 used the Joint Phases of Operations as

its basis and was completed in May 2013. The ANA 3.0, currently in the planning stage, intends to incorporate several major strategic initiatives.

It is critical that we continue to keep the ANA current. The pace of technology today is staggering. As soon as you buy the latest widget and understand how to use it efficiently, you find yourself bombarded with advertisements for the new and improved version coming out. That raises another important issue of compatibility. Army networks consist of different versions of products that must be able to interoperate seamlessly. An updated ANA ensures the product you derive from referencing it will be able to interface and keep pace with technology and evolving Army networks.

The U.S. Army Signal Regiment consists of many moving parts. The mission is fast paced, complex and focused on technology. It requires Soldiers who are network savvy, customer oriented and tactically proficient. However, there are other issues besides satellites, routers or radios that have a profound effect on the conduct of our business. The changes caused by this effect have to be accounted for in the ANA or it is no longer a viable reference architecture.

The organizational design and mission of Signal Corps

(Continued on page 20)

(Continued from page 19)

units influences the ANA. If there are changes in the organizational design of these units due to Force Design Updates, the ANA has to be adjusted. When higher level command decisions are made regarding manning, resourcing and or capabilities, the impact of these decisions can be far reaching and the ANA has to be updated accordingly. The composition and mission of the units dictates the Information Exchange Requirements they perform. The IERs are critical to the design of the ANA.

Doctrine can have a profound influence on the ANA. Documents are always being created, revised, recently approved or coming up for review. The ANA must be updated periodically to keep pace with these doctrinal changes. The Signal Regiment has a few key documents in the pipeline currently. Some examples are: The Integrated Tactical Network Environment Concept of Operations, FM 6-02 Signal Support to Operations, Army Techniques Publications 6-02.71 NetOps, the Army Enterprise NetOps CONOPS, and the Army Expeditionary NetOps CONOPS, to name a few.

In order to provide the Warfighter with an integrated network that enhances Mission Command and enhances their ability to accomplish the mission, communications need to be robust, reliable and available. The ANA

is a key component in making that a reality. For the ANA to remain a relevant Reference Architecture, it must be regularly updated and used by the U.S. Army Signal Regiment/ military information technology community in the design of future communications networks. The ANA can be found at the Army Capability-based Architecture Development and Integration Environment website: <https://cadie.army.mil/Cadie/ArchCatalog/Registration.aspx?ArchitectureId=554>.

Terry K. Dawkins is a Senior Cyber Network Operations Analyst at TRADOC Capability Manager, Global Network Enterprise. He began his military career as a private in the Army Signal Corps in 1989 and retired as a first sergeant in 2009. He served 20 years on active duty in Germany, Kosovo, Iraq and several stateside tours.

Derrick J. Smith is the Principle LWN Enterprise Architect at TRADOC Capability Manager, Global Network Enterprise. He began his military career as a private in the Army Medical Corps in 1981 and retired as a Signal Corps lieutenant colonel in 2009. He served 24 years on active duty in Germany, Saudi Arabia, Korea, Belgium, Afghanistan, Kuwait and several stateside tours. He also served three years in the U. S. Army Reserves and one year in the Florida Army National Guard.

ACRONYM QuickScan

ANA - Army NetOps Architecture
AR - Army Regulation
ARCYBER - U. S. Army Cyber Command
ARNG - Army National Guard
ARNGUS - Army National Guard of the United States
CIO - Chief Information Officer
CONOPS - Concept of Operations
DCO - Defensive Cyber Operations
DoD - Department of Defense
DoDIN - Department of Defense Information Networks
DOTMLPF-P - Doctrine, Organization, Training, Materiel, Leadership, Personnel, Facility-Policy

FM - Field Manual
IER - Information Exchange Requirements
ITNE - Integrated Tactical Network Environment
JIE - Joint Information Environment
LWN - LandWarNet
NetOps - Network Operations
OCO - Offensive Cyber Operations
TCM GNE - TRADOC Capability Manager for Global Network Enterprise
TRADOC - U. S. Army Training and Doctrine Command
WIN-T - Warfighter Information Network-Tactical
USAR - U. S. Army Reserve

1st Cyber Network Defender specialists graduate

By Wilson A. Rivera

Fifteen Soldiers made history when they were awarded the newest Army military occupational specialty, 25D, cyber network defender, during a graduation ceremony 27 Nov 2013 held in Alexander Hall at Fort Gordon, Ga.

Soldiers completed a 14-week course, dubbed as rigorous for its curriculum, to learn the skills needed to meet the demand for cyber warfare.

"Cyberspace is composed of hundreds of thousands interconnecting computers, servers, routers, switches, fiber optic cables which allow our critical infrastructure to work," said CSM Ronald S. Pflieger, regimental sergeant major for the U.S. Army Signal Center of Excellence and Fort Gordon, guest speaker for the first-ever graduating class for the Cyber

Network Defender course.

"With the need for educated individuals to defend our network, so does the need to engage cyberspace," CSM Pflieger said.

Through the establishment of the new cyber network defender, 25D, MOS, there were changes made to the classification and structure among the 25 career management field series for communications and information systems operation with other MOS revisions of information technology specialist, 25B; radio operator-maintainer, 25C; and telecommunications operator chief, 25W.

Significant changes to the 25 CMF identify the positions and personnel to perform duties with cyber network defense, and selected functions for cyber network defender MOS positions transferred

from previous MOS positions associated with cyber network defense.

Major duties a cyber network defender will perform include protecting, monitoring, detecting, analyzing, and responding to unauthorized cyberspace domain actions; deployment and administration of computer network defense infrastructures such as firewalls, intrusion detection systems and more. Soldiers are also tasked to take action to modify information systems, computer network configurations in regard to computer network threats and collect data to analyze events and warn of attacks. Cyber network defenders will be trained to perform assessments of threats and vulnerabilities within the network environment, conduct network damage assessments, and develop response actions. Staff sergeants interested in becoming a cyber network defender must meet requirements such as having a minimum of four years information technology experience, an ASVAB of 105 in both their GT and ST scores. They must be a U.S. citizen, complete an in-service screening, a recommendation from their battalion or higher.

For more information about requirements, visit <https://www.us.army.mil/suite/page/838>.



Graduates of the first Cyber Network Defender Military Occupational Specialty participate in graduation ceremonies on 27 Nov 2013 at Fort Gordon, Ga.

Wilson Rivera is editor of the Signal Newspaper at Fort Gordon, Ga.

Tactical Public Key Infrastructure Concept of Operations published

By Michael Jones and Jimmy Kilgore

The Signal Center of Excellence commanding general approved a concept of operations for Tactical Public Key Infrastructure dated 5 June 2013.

The CONOP is designed to outline the Army's concept for employing PKI in tactical environments, to include Secret Internet Protocol Router Network and Non-classified Internet Protocol Router Network for tactical elements operating at any location from home station to deployment in support of Combatant Commands. The TPKEI CONOPS documents the concept for TPKEI as an extension of the existing Department of Defense and Federal PKI services to meet Army operating forces' cryptographic security needs.

The extension of these services provides the Warfighter with the ability to securely authenticate to and securely communicate with tactical resources as well as other resources across the Department of Defense Information Networks. TPKEI will support registration of tactical subscribers (i.e. users), issuance of NIPRNet Common Access Cards, SIPRNet Tokens and Non-Person Entity or "device" certificates.

In conjunction with directory services, tokens and PK-enabled applications, TPKEI will provide the framework and systems required to perform cryptographically based data integrity, authentication for network access control, data confidentiality and non-repudiation services. The TPKEI CONOPS, which you can download at <https://tiny.army.mil/R/VQMS/>, describes the roles, responsibilities and relationships of systems

and personnel and how the Army plans to implement PKI in tactical units.

Policy

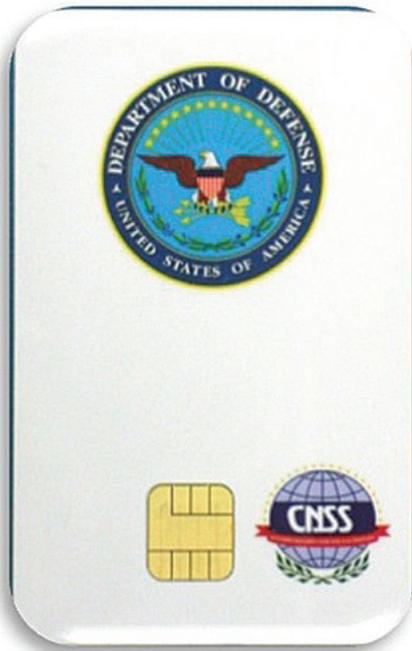
The DoD Chief Information Officer has mandated the use of a PKI hardware token on both the NIPRNet and SIPRNet to eliminate anonymity and improve the security of these networks.

This provides greater security over username and password. With network access based on a PKI hardware token, it will be much harder for adversaries to access the DoDIN and the information and resources contained on it.

NIPRNet Common Access Card

As you probably know, the DoD-issued CAC is the primary identification card for Army Soldiers, Department of the Army Civilians, and contractors, and is the primary DoD PKI hardware token used on the NIPRNet.

The principal mechanism for CAC issuance is the deployable Real-time Automated Personnel Identification System workstation, which queries the Defense Enrollment Eligibility Reporting System database to verify the intended cardholder's identity. The tactical NIPRNet token (i.e. CAC) issuance process is managed by G-1/S-1 sections. Soldiers assigned to the Corps G-1, Division G-1, and Brigade Combat Team or Multifunctional Brigade S-1, serving as Verifying Officials, manage CAC issuance utilizing the RAPIDS Workstation to issue, reissue, and revoke NIPRNet CACs and perform Personal Identification Number resets. None of these



(CAC) Token Issuance

functions can be performed in a disconnected environment--they require connection to the NIPRNet.

While in Garrison, the deployable RAPIDS

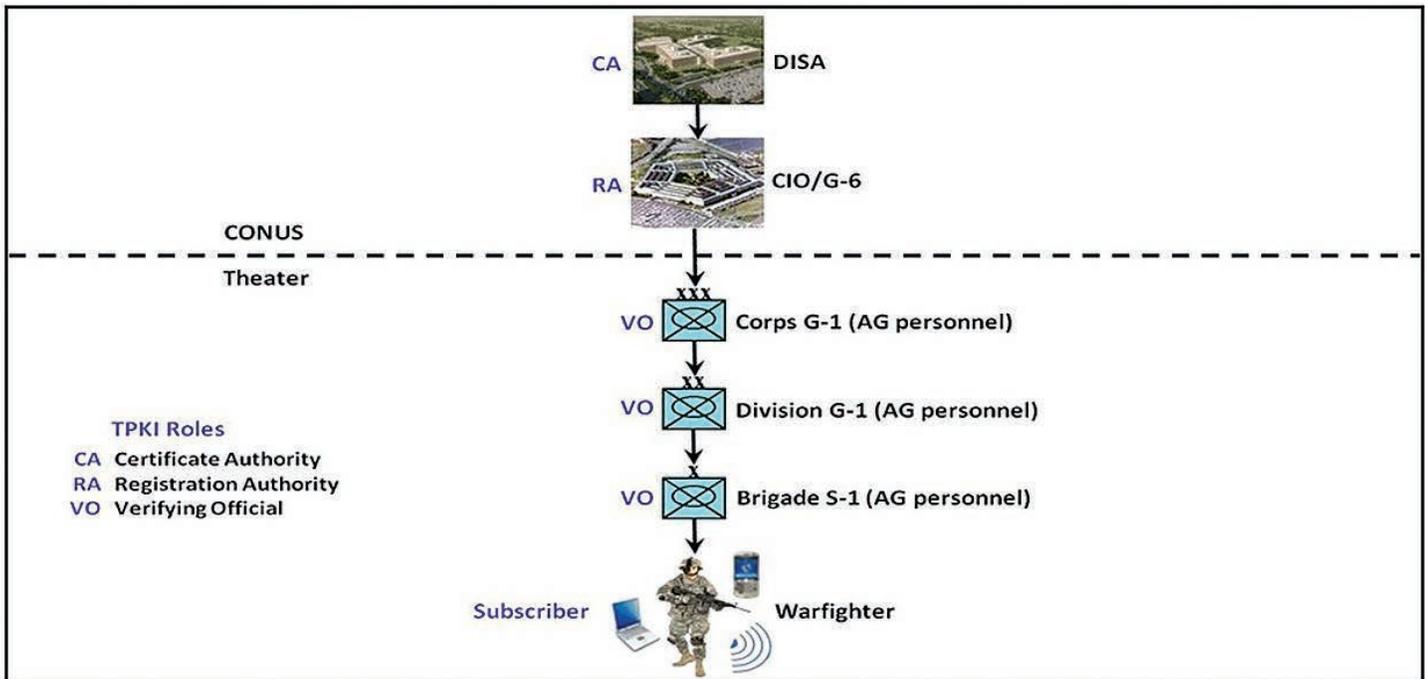
workstation located at the Brigade S1 connects to the installation NIPRNet to access the Certificate Authorities in the Contiguous United States. While deployed, it typically connects over a "stove pipe" commercial Very Small Aperture Terminal satellite terminal issued with each deployable RAPIDS workstation. This system carries with it a huge monetary burden for lease of the equipment, satellite airtime, maintenance and customer support. SIGCoE TRADOC Capability Manager for the Global Network Enterprise, along with the Communications-Electronics Research, Development and Engineering Center, and the 35th Signal Brigade's 63rd Expeditionary Signal Battalion, have conducted DEERS/RAPIDS CAC PKI

operations testing over a NIPRNet connection provided by a WIN-T tactical network. The results of this testing showed that the DEERS/RAPIDS tasks and activities worked successfully over WIN-T. We were able to issue CACs and reset CAC PINs via the tactical network connection over the course of several test events. With these positive results, current budget constraints, and the Army's "Single Network Concept," removing the VSAT system from the Brigade S1 is being considered.

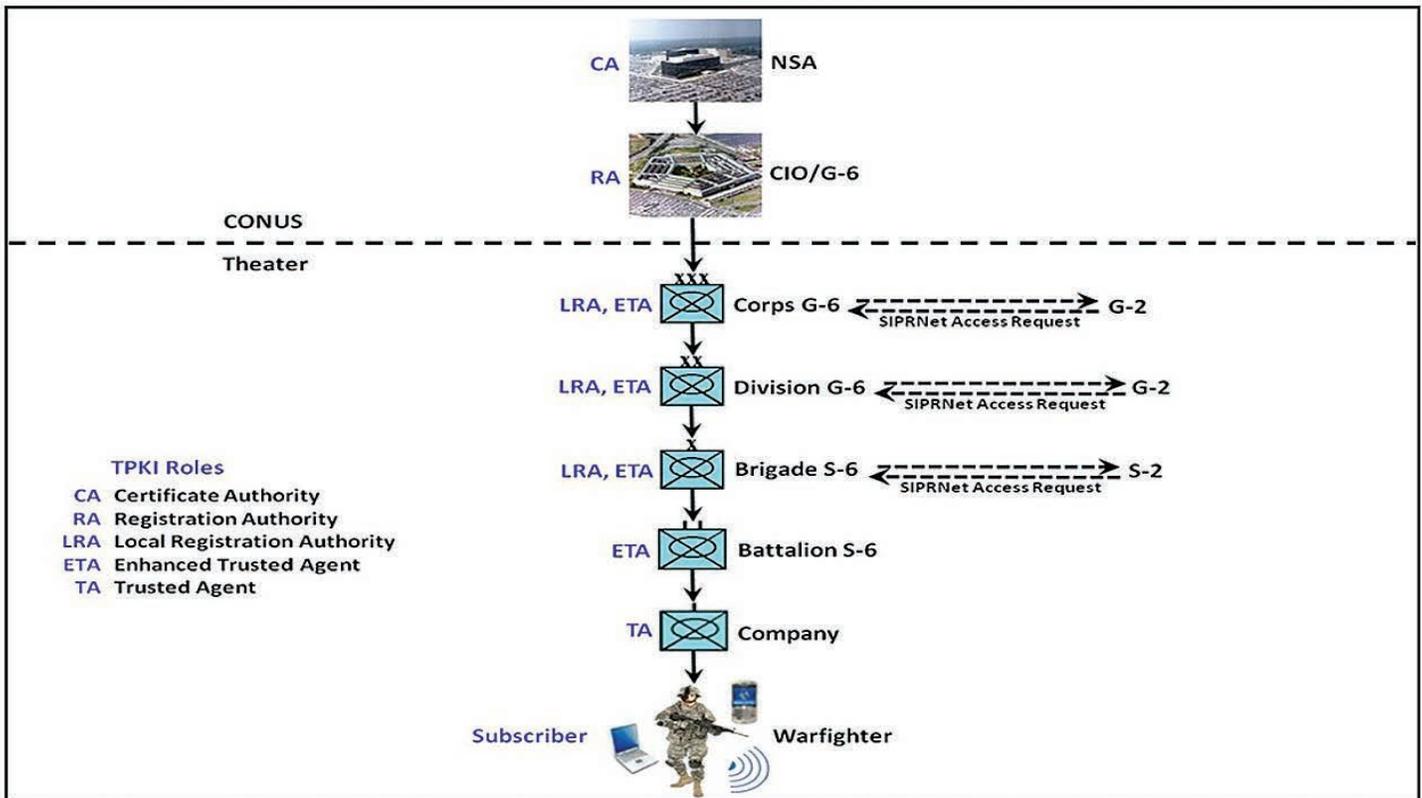
SIPRNet Token

The primary DoD PKI hardware token used on the SIPRNet is the SIPRNet Token. Similar to the CAC, the SIPRNet Token contains

(Continued on page 24)



Tactical NIPRNET Token (CAC) Issuance



Tactical SIPRNET Token Issuance

(Continued from page 23)

certificates used only for logical network access, digitally signing, and encryption.

Unlike the multi-purpose CAC, the SIPRNet Token is not an identification card; it does not bear a photo of the subscriber, fingerprint or other personal information. Because the SIPRNet Token is not an ID card, the issuance process will be different from that for the CAC. The issuance procedures for SIPRNet Tokens are performed on a Certificate Issuance Workstation, also called a Local Registration Authority workstation, and managed by the Corps G6, Division G6, and the Brigade S6, not the

G-1/S-1.

Signal Soldiers assigned to the BCT or Multifunctional Brigade S-6, serving as LRAs, Trusted Agents, or Enhanced Trusted Agents, will manage SIPRNet Token issuance utilizing the LRA workstation. TCM GNE, along with the Communications-Electronics Research, Development and Engineering Center Space & Terrestrial Communications Directorate Cyber Security Information Assurance Division, has tested the ability to issue SIPRNet Tokens on a tactical, bandwidth-constrained WIN-T network and successfully issued SIPRNet hardware tokens without any significant issues.

The CIW interacts and talks with the Web-based

Token Management System in CONUS, which manages the SIPRNet Token issuance process. The CIW is used to perform the following functions: 1) Formatting "New" cards for first time use, 2) Reformatting a used card for a new user, 3) Resetting PINs, when forgotten and/or blocked for too many PIN entry attempts, 4) Re-enrolling the card when changing users, and 5) Displaying information



Non-person entity devices

about the card and certificates on the card.

Similar in many ways to Communications Security key management, Signal Soldiers assigned to the Brigade S-6 Information Assurance/Computer Network Defense Section will likely manage certificate issuance at the BCT brigade and battalion level. At the company level, where there is only one Signal Soldier currently authorized, the Signal Support Systems Specialist will perform TA duties. Note: The use of a TA or ETA at the battalion and company level are dependent upon the type of unit, the unit's staffing and the corresponding density of Soldiers that require use of a SIPRNet Token. Some units may elect to not use either position at the company level and only conduct SIPRNet Token issuance and sustainment operations from the brigade or battalion level.

Tactical SIPRNet Token Issuance

A user (i.e. Soldier) in a deployed BCT who needs a SIPRNet Token issued will go to their local company or battalion ETA/TA, or an LRA at brigade, division, or corps, and submit a request for SIPRNet access. As shown by the dotted arrows between the S6/G6 and the S2/G2 in the above figure, the company or battalion ETA/TA will submit the request to the brigade S6 LRA or ETA, who will submit it to the brigade S2 or commander for approval. The TPKI CONOPS provides more detail.

Non-Person Entity

In addition to enabling secure authentication for person entities, TPKI will provide software certificates for authentication of Non-Person Entities. NPEs are non-humans, such as computers, operating systems, applications, services and devices like routers and switches. The Corps G6, Division G6, and Brigade S6 will be responsible for NPE certificate management. Signal Soldiers assigned to the BCT or Multifunctional Brigade S-6, serving as NPE Sponsors and NPE Verifying Officials, will manage NPE certificate issuance at the brigade utilizing a

forthcoming NPE management solution.

Since the NPE Sponsor acts on behalf of the NPE in order to obtain a PKI certificate, this role should probably be filled by the S-6 Soldier(s) responsible for the administration, configuration, and operation of the NPE devices, services or applications. The DoD is currently working to select an NPE management solution for DoD Services and Agencies that will support auto-enrollment and auto-renewal to make the management of these certificates easier.

In order to provide software certificates to NPEs, two independent TPKIs will be established. The first is a Medium Assurance NPE, which utilizes the DoD PKI root with strict policy requirements and, therefore, a higher trust between devices, but is more difficult to implement in a tactical environment.

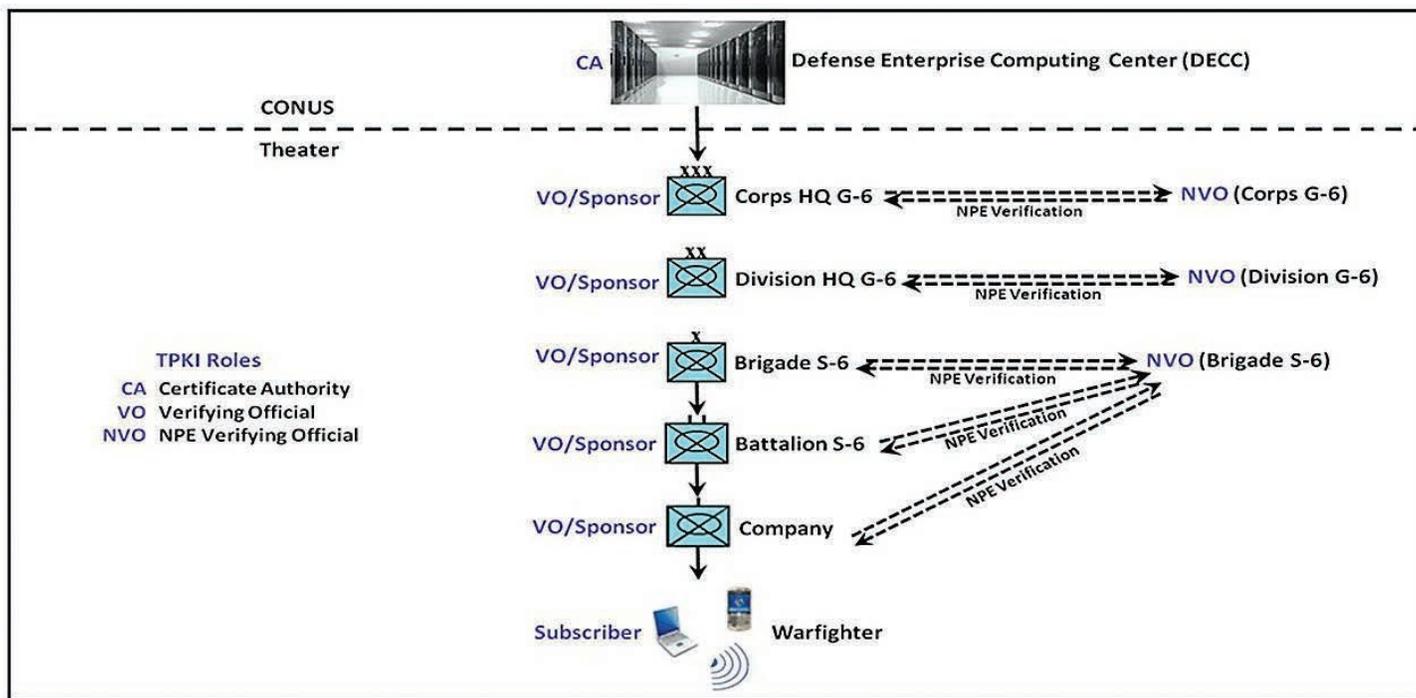
The second will be the Less Than Medium Assurance NPE, which will utilize a Service-oriented (Army) root to establish a Deployed CA. The LTMANPE is less secure, but easier to implement (i.e. less restrictions), and will allow computers, applications and devices to be dynamically issued credentials that will enable secure connections to the tactical network and between tactical entities in the unit, creating a secure Network Operations environment.

This allows the NPE to auto-enroll or obtain its own certificates, which helps reduce the manual labor needed to manage the millions of devices within the Army.

TPKI and the Network

A critical component of PKI is the necessity to check to see if a certificate has been revoked. A Certificate Revocation List is a file, published by the CAs, which contains the lists of revoked certificates. DoD CRLs are hosted on the Global Directory Service and are available on NIPRNet and SIPRNet. A complete CRL contains the entire list

(Continued on page 26)



NPE Software Certificate Issuance Medium Assurance

(Continued from page 25)

of revoked certificates for all certificates issued by that CA. In tactical, bandwidth-constrained environments, a full CRL can take an excessive amount of time to download. The ability to distribute CRLs throughout the DoD environment is increasingly being challenged because the size of the CRL affects the ability of relying parties (persons or NPEs using the certificate) to download the CRLs, typically due to clogging of available resource bandwidth. Implementation of TPKE over WIN-T introduces technical challenges for PKI certificate validation due to lower bandwidth and higher latency than on strategic networks.

To overcome these challenges, CERDEC S&TCD CSIAD engineers have been testing possible solutions for increasing performance of PKI certificate validation services over WIN-T at the brigade and battalion level. These solutions include using alternate formats for the revocation lists and placing PKI infrastructure, such as OCSP repeaters

and responders, at the brigade level. Testing results influenced development of the TPKE CONOPS and will help identify an optimal solution for distributing certificate revocation information to tactical systems, as well as to inform Army policy, requirements, Tactics, Techniques and Procedures, and configuration Best Business Practices for the implementation and deployment of PKI validation services within the Army tactical environment.

Conclusion

Looking ahead, TCM GNE, along with our SIGCoE and Army partners, will continue capabilities development and planning efforts towards implementation of TPKE.

Analysis is ongoing to determine potential impacts and actions necessary in the areas of doctrine, organization, training, materiel, leadership, personnel, and facilities. This analysis will address some details of TPKE implementation that were outside the scope of the CONOPS.

Testing of TPKE certificate validation

alternatives is ongoing and the results will help determine the solution chosen for implementation.

Regardless of the specific solution chosen, one thing is certain: TPKE will enhance the security and safety of Army computer networks by establishing an integrated capability that provides network access control, minimizes insider threats, and

audits user activities across the cyber domains.

Michael A. Jones presently works as an Army contractor in support of the TCM GNE Network Assurance Section, U.S. Army Signal Center of Excellence at Fort Gordon, Ga. He is a retired Information Technology Specialist (MOS 25B) Signal Soldier with five years' experience as an Army

Network Assurance capabilities developer.

Jimmy L. Kilgore presently works as an Army contractor in support of the TCM GNE Network Assurance Section, U.S. Army Signal Center of Excellence at Fort Gordon. He is a retired Signal Support Systems Specialist (MOS 25U) Signal Soldier with three years' experience as an Army Network Assurance capabilities developer.

ACRONYM QuickScan

BCT – Brigade Combat Team
CA – Certificate Authority
CAC – Common Access Card
CERDEC – Communications-Electronics Research, Development and Engineering Center
CIO – Chief Information Officer
CIW – Certificate Issuance Workstation
COCOM – Combatant Command
CONOPS – Concept of Operations
CONUS – Contiguous United States
CRL – Certificate Revocation List
CSIAD – Cyber Security Information Assurance Division
DAC – Department of the Army Civilians
DEERS – Defense Enrollment Eligibility Reporting System
DoD – Department of Defense
DoDIN – Department of Defense Information Networks
DOTMLPF – Doctrine, Organization, Training, Materiel, Leadership, Personnel, and Facilities
ETA – Enhanced Trusted Agent
IA/CND – Information Assurance/Computer Network Defense
LRA – Local Registration Authority

LTMANPE – Less Than Medium Assurance NPE
NIPRNet – Non-classified Internet Protocol Router Network
NPE – Non-Person Entity
NSA – National Security Agency
OCSP – Online Certificate Status Protocol
PIN – Personal Identification Number
PKI – Public Key Infrastructure
RAPIDS – Real-time Automated Personnel Identification System
S&TCD – Space & Terrestrial Communications Directorate
SIGCoE – Signal Center of Excellence
SIPRNet – Secret Internet Protocol Router Network
TA – Trusted Agent
TCM GNE – TRADOC Capability Manager for the Global Network Enterprise
TMS – Token Management System
TPKI – Tactical Public Key Infrastructure
VO – Verifying Official
VSAT – Very Small Aperture Terminal
WIN-T – Warfighter Information Network-Tactical

Active shooter architecture approach offers joint operations protection

By LTC Phillip G. Burns

A proposed Logical Active Shooter architecture can form the operational basis to secure critical information systems from malicious access in joint operation environments.

Everyone involved with cyber operations knows that America and our allies face continually escalating cyber threats to national interests. Unfortunately the pool of security professionals who are able to operate effectively in cyberspace is not very deep.

This lack of sufficient numbers of trained cyber defense professionals is the weakest link in the current network defense chain.

A study by Frost and Sullivan supports this assertion (Frost and Sullivan, "The 2011(ISC) 2 Global Information Security Workforce Study." 13 May 2013 https://www.isc2.org/uploadedFiles/Industry_Resources/FS_WP_ISC%20Study_020811_MLW_Web.pdf).

In addition, many of today's cyber security professionals can be considered digital immigrants who must learn about the digital environment and its threats.

On the other hand, digital natives are individuals who grew up with computers, video games and computer graphics. Automation is second nature to digital natives.

Department of Defense organizations, such as U.S. Cyber Command and the National Security Agency, must reach out to digital natives, recruiting and molding them to hunt for malicious intruders, build and defend the military network.

Of course, distinctions between U. S. Code Title 10 and USC Title 50 [2] – between operations and intelligence – may constrain how we hunt for adversaries, build and defend the network. (Wall, Andru. "Demystifying the Title 10-Title 50 Debate: Distinguishing Military Operations, Intelligence Activities & Covert Action." Harvard National Security Journal 3 (2011).)

According to Andru Wall, decisions to execute a defense against a cyber attack are often measured in seconds or milliseconds. Operators placed in the frontline defender position must have Title 10/50 authorities and the ability to make decisions locally, to apply operational

effects necessary to protect or isolate the network. This ability to make quick decisions is a learned skill that adds to the challenges of network defense.

As USCYBERCOM and NSA focus on building the bench of cyber security professionals, measures must be in place to protect information as the gap decreases between digital natives and digital immigrants. Until the bench is built, the focus must be to secure data, but not overly restrict the DoD users' access to data in a manner that prevents collaboration.

Within the scope of this discussion, the DoD is directing the consolidation of disparate data centers across the DoD network to a select set of core data centers. Efforts will lead to the integration of the Army's portion of the DoD network with the Joint Information Environment at Figure 1. The JIE will provide a single network that is secure, standards-based, and flexible. The JIE must also support versatile mission sets according to LTG Susan Lawrence. (Lawrence, Susan. "Network Information Brief: Improving

Network Security and Operational Effectiveness.”
 7 June 2012 http://ciog6.army.mil/LinkClick.aspx?fileticket=O4Ezkdq_fGU%3D&tabid=36.)

Future Army network capabilities include chat services and software defined radios that, in accordance with the Unified Compliance Framework, will connect users at home or work with deployed enterprise users.

As Figure 1 indicates, all are geared to ensure enterprise users have the “...information they need, when they need it, in any environment, to manage the Army Enterprise and enable Full-Spectrum Operations with our Joint, Coalition, and Interagency partners,” said LTG Lawrence. JIE will usher unprecedented access to

information and a new era of collaboration and situational awareness that enable Mission Command formidable network and technology tools.

While JIE will provide the standards and the common environment, the services will employ technologies, such as Host Based Security System, Public Key Infrastructure, Rights and Identity Management, to assure confidentiality, integrity and availability of information; however, these technologies alone may not foster a completely secure environment. The Deployed Environment and Defense Information Systems Network clouds at Figure 1 typify one-to-many user interactions, which may be difficult but not impossible to audit.

This article focuses on

logically and physically securing critical DoD information with limited impact to users’ experience and collaborative efforts to ensure situational awareness critical to Mission Command. This article explores a Logical Active Shooter System that ensures data is protected from unintentional or intentional spillage. The system must support Title 10/50 requirements, while simultaneously restricting the digital native’s ability to circumvent its controls. The Bradley Manning incident (i.e., “Wikileaks”) is mentioned as a useful case study.

The Logical Active Shooter System

U.S. Army Mission Command Center of Excellence’s Requirement Governance Team, in coordination with U.S. Army Signal CoE’s TRADOC Capability Manager for Global Network Enterprise, are developing an operational framework for a cloud-based computing network. Figure 2 illustrates a proposed operational view underpinning the principles of this cloud-based computing network. (Mackert, Donald. “Cloud Computing Operational View 1 from the Data Center to the Tactical Edge.” (email communication,

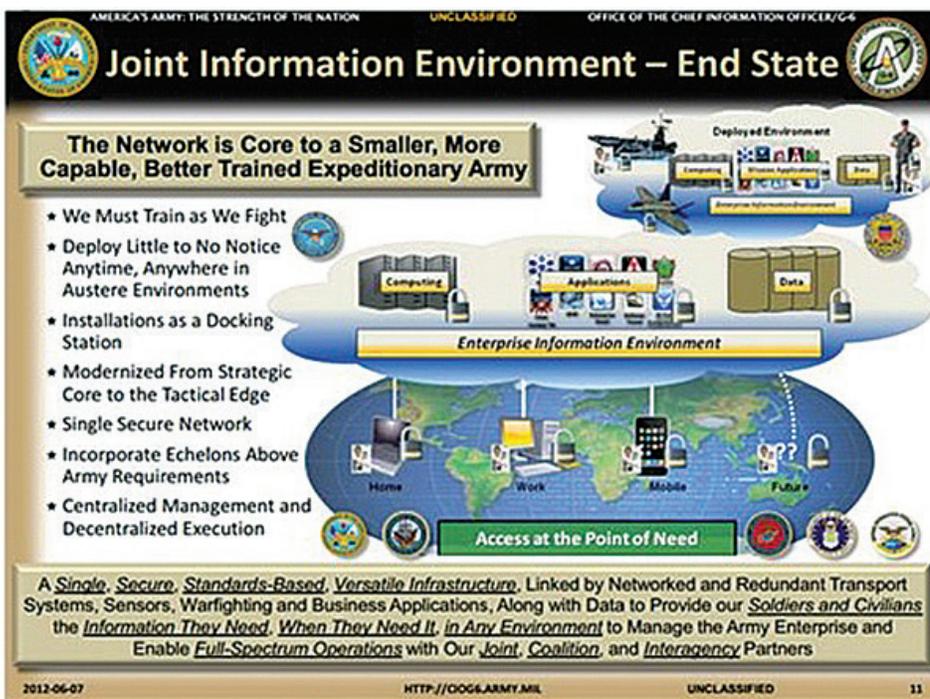


Figure 1. The Joint Information Environment – End State

(Continued on page 30)

9 April 2013)). Deployment of the Logical Active Shooter System would occur after the JIE end state as illustrated in Figure 1.

Security technologies, such as HBSS, PKI, and Rights and Identity Management, will be critical to the future network and engineered in the architecture from the start to ensure the end state of a "Single Secure Network." The DoD and Army cloud-based computing networks will leverage the National Institute of Standards and Technology definition of cloud computing:

"...a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction." (Mell, Peter, et. al. "The NIST Definition of Cloud Computing: Recommendations of the National Institute of Science and Technology." September 2011 <http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf>).

The NIST definition implies that anonymous access to information is expected; however, shared concerns of mission security requirements, policy, and

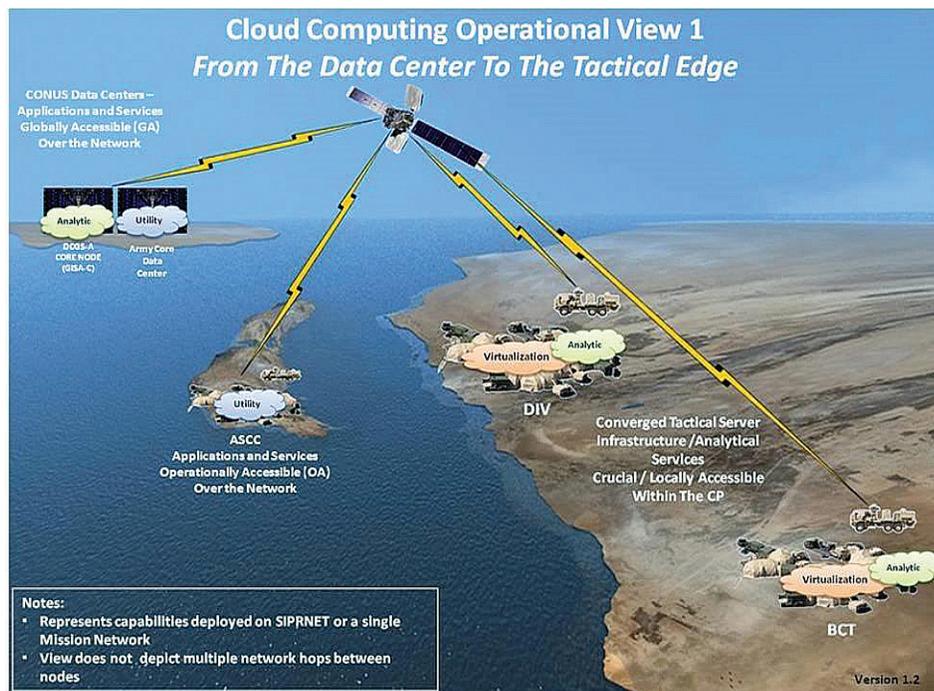


Figure 2. Cloud Computing Operational View

compliance considerations will be factored into instantiations of a cloud-based computing environment. Within a deployed setting, loss of data or spillage of classified material is a real concern, and anonymous access is hard to monitor.

It takes leadership and active participation of users to enable an environment where mission critical information is secured from unauthorized users and access.

The Bradley Manning incident illustrates the complexity of preventing the spillage of classified material.

The Bradley Manning incident serves as a stark reminder of what happens when lax security posture and uninvolved leadership intersect.

Bradley Manning was a digital native who represented

a class of insider threat (a disgruntled employee who displays some emotional distress). He pled guilty to mishandling classified materials and uploading information to WikiLeaks.org via his personal laptop. To mitigate situations like this, an 'active shooter'-like stance or posture is needed.

Technical controls are required and in some cases are implemented, but to what degree of success are debatable. Furthermore, involvement of leadership helps to improve IT security, and a well-informed IT security staff helps to identify and correct situations.

Taking an active shooter-like stance is to intercept the malicious attacker while he or she is in the process of executing the attack on the network or information

system. This stance can be via involvement of leadership/fellow users or automated enforcement of rules and roles.

An active shooter-like stance alone will not in itself adequately protect the DoD network and mission critical information, because the distributed and open-access nature of cloud computing injects a level of risk that must be factored into risk assessments and technical controls. A roles-and-rules based system is needed to adjudicate or restrict access.

Figure 3 illustrates a recommended capability that can secure critical information and logically establish an

active shooter capability.

For the purpose of this article, critical information is defined as information that enables situational awareness within a mission setting that includes classified or For Official Use Only information where its unintended release or leakage impacts a mission or strategic aims. Information releasable to the public is not defined as critical information that will be protected.

The first step is to adjudicate access based upon established roles- and rules-based policies, to which users can authenticate through technology such as Rights Management or PKI. The goal is to marry roles-and-rules

based access to the specific platform where access was initially generated. This would be a goal at end state. This is decision point #1 as illustrated in Figure 3. If access to information enables collaboration in support of mission informational and situational awareness requirements, then DP2 is enabled. If identity is not verified, then access to information is terminated. Levels of access to information under DP2 are determined by roles-and-rules based access requirements. Information can be in the form of voice, video, and data. Access to data files is time limited and files are automatically shredded to keep information relevant and current. Timeframes for access to data file are determined by the data owners.

If the answer to DP1 is no, then DP3 is enacted, and the user's identity is verified. Once the user's identity is verified, then the user has access to non-mission critical information only; screenshots of websites are prohibited; and data files are set to time out to ensure information is relevant and current. If the user's access under DP3 cannot be verified, then access to information under this category is terminated.

There are several technologies that can enable the capability represented in

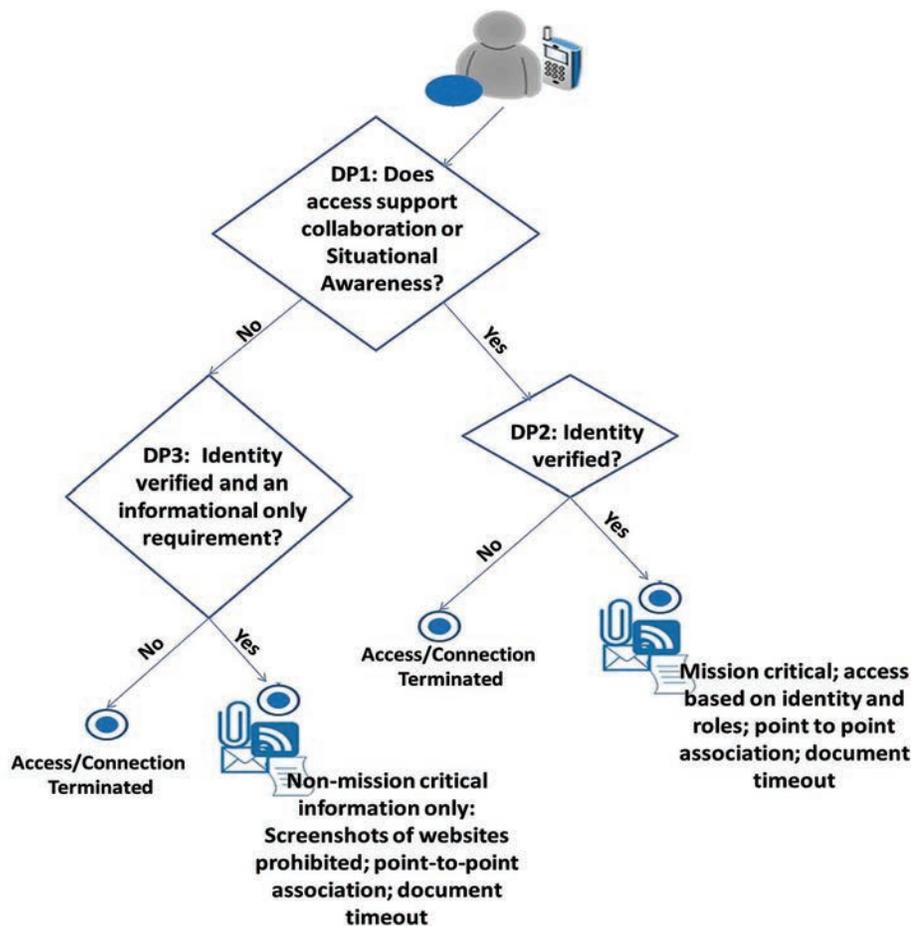


Figure 3. User Data/Chat/Voice/Video Access

(Continued on page 32)

Figure 3. Potential document security solutions should include desired characteristics vital to securing critical information as defined above, which includes lifecycle management of critical documents.

To narrow the scope, solution sets should support refinement of critical characteristics of the Logical Active Shooter System: role- and rule-based access; a virtual workplace where documents are shredded, encrypted, and interleaved upon termination of connection to the virtual workplace; supports bandwidth constrained environment.

If we analyze Figure 3 in greater detail, additional system attributes and capabilities emerge and can be discussed as a refined system as shown in Figure 4.

Figure 3 initially depicts a capability where the ability to authenticate access and contain access is based upon roles and established rules. Updated information is continuously rendered to the user, and a dynamic auditing capability is enabled to scope future access based upon the informational needs of the user. Users do not directly access secured material. Users request access to a particular document and a secured, virtual workplace

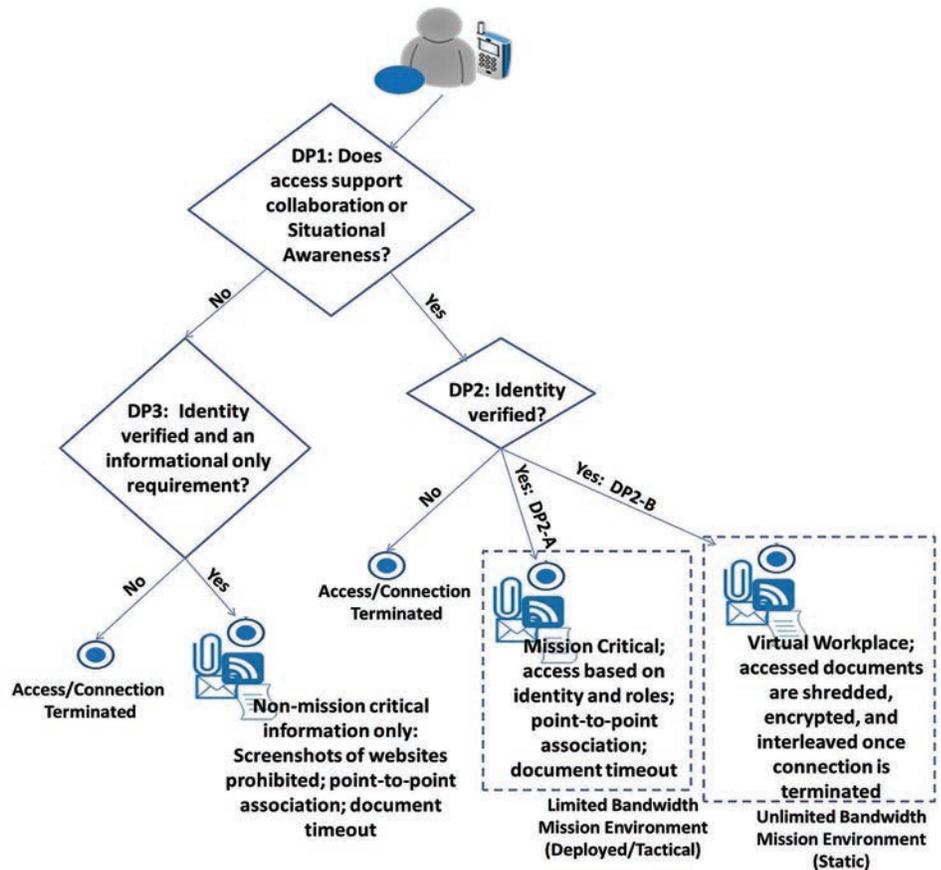


Figure 4. User Data/Chat/Voice/Video Access

is created via a protected tunnel. This virtual workplace facilitates tracking, queuing, and securing of document requests. In addition, this capability must support users' to access current information every time documents are introduced to their workplace. A proposed capability must ensure that once documents are saved and closed they are logically shredded, encrypted, and interleaved with white noise before being scattered randomly throughout the storage environment within the cloud architecture. Doing this reduces attack threat vector considerably, raising

information protection to a new level.

While one goal of the JIE is to eventually virtualize Joint common services, tactical users must have access to critical information even while not connected to the DISN. Therefore, an additional critical need for the system is to ensure that a common operating picture is available to the war fighter and commander in a degraded or disconnected environment. Situational awareness data and collaborative services in support of missions must go unfettered throughout the Joint phases of the operation.

Selected capabilities must support this critical need in addition to securing critical information from malicious exfiltration or willful disclosure of critical information.

An inclusion of a final requirement is access validation through Rights Management, PKI, and Active Directory is a final critical enabler to DP1. DP2 is divided into two sequels: DP2-A and DP2-B. DP2-A supports users in a band- width constrained environment, or users who will be adversely impacted if disconnected from the DISN. Therefore, DP2-A provides access to mission critical information with point-to-point association and document timeout to ensure information is current. DP2-B will support user's access to critical information when bandwidth and potential disconnection from the DISN is not an overarching concern. DP2-B provides a virtual workplace that facilitates

access to mission critical information.

Figure 4 provides an updated view of the proposed Logical Active Shooter System after enumerating additional requirements proposed in Figure 3.

Conclusion

The two Logical Active Shooter System solutions described in this article are only the tip of the iceberg of capabilities that DoD can leverage. They provide a referential architecture that can support a secure cloud-based network. Both capabilities can go far to mitigate an insider threat like Bradley Manning. With the recent posturing and alleged hacking exploits by the Democratic People's Republic of Korea, the need to secure information against all threats becomes paramount as we develop and migrate to a Joint Information Environment. If an organization takes an appropriate active shooter-like

stance, then the insider threat (intentional or unintentional) can be effectively mitigated. A logical means of bolstering this "active shooter"- like stance is needed to secure critical information and limit exploitation of critical information by insider and outsider threats.

LTC Phillip G. Burns is currently a NATO staff officer. Prior to his current assignment, LTC Burns served as a capability manager for the U.S. Army Signal Center of Excellence. Prior to that, he served as the Information Assurance Officer for the 2nd Infantry Division, Camp Red Cloud, South Korea. He holds a Master of Science in Computer Information Systems. In 2007, he graduated from the Information Systems Officer course at the U.S. Army's School of Information Technology at Fort Gordon, Ga.

Join the Discussion

<https://SIGKN.army.mil>



ACRONYM QuickScan

DoD - Department of Defense

DoDIN - Department of Defense Information Networks

HBSS - Host-Based Security System

IT - Information Technology

JIE - Joint Information Enterprise

NIST - National Institute of Standards and Technology

NSA - National Security Agency

PKI - Public Key Infrastructure

SIGCoE - Signal Center of Excellence

USCYBERCOM - U.S. Cyber Command

Army leaders taking holistic approach to simplifying network operations

By Amy Walker

The suite of network management tools provided by the Army's tactical communications network backbone, Warfighter Information Network-Tactical, provides today's signal officers with the "big picture" of the network so they can maximize its power and keep Soldiers connected.

An advanced version of these Network Operations tools will also serve as a standard baseline as the Army takes a more holistic view of the network and moves to

eliminate disparate NetOps tool sets from various systems and domains.

"Today's WIN-T NetOps give us a lot more power to reach into the network and control everything from a central location, with line-of-sight or satellite networks," said Maj. Graham Wood, the communications officer for the Army's 3rd Brigade Combat Team, 10th Mountain Division (Light Infantry). "There is a huge density of systems now, so being able to manage them from one location becomes a necessity."

Newly deployed WIN-T

NetOps capabilities are supporting S6s in theater as they facilitate the planning, initialization, monitoring, management and response of the network. They enable these communication officers to identify how well their systems are actually working on the battlefield, so as units move out in any direction, they have the ability to "see" different enclaves within that unit.

"The WIN-T NetOps tools give us a really good idea as to the health of our network, what it looks like, what kind of bandwidth we're using



(U.S. Army photo by SPC Edward Bates)

A Soldier checks a Warfighter Information Network-Tactical Increment 2 Point of Presence-equipped vehicle at Forward Operating Base Gamberi, Afghanistan, in September 2013. Communications officers in theater use WIN-T Increment 2 Network Operations tools to display the geographical position of these and other communications nodes, as well as network strength and how well the systems are working, whether stationary or on-the-move.

as far as our throughput, and that helps us with our overall network analysis," said Maj. Ernest Tornabell, 2nd Brigade, 1st Armored Division brigade S6, who uses WIN-T Increment 2 during the Army's Network Integration Evaluations. "With this network management suite, it's like turning on a light bulb; where you didn't have that visibility into the network before, now you do."

Inside a network operations and security center, WIN-T NetOps display maneuver elements on the battlefield (such as dismounted infantry, fires or aviation) on a large screen for easy monitoring. Not only does the NetOps capability display a particular system or node's geographical position, it also shows network strength and how well the system is working, whether stationary or on-the-move. Being able to watch the physical location of a node on a map, see how it is moving, and how it is dropping and gaining links enables the S6 to help the brigades or battalions troubleshoot potential issues and fix them before they arise.

"Some of the NetOps tools provide a warning of impending issues," Wood said. "We are able to notice things and contact the unit by means that are still available and help get that link tuned properly before it drops."

The tools can also prioritize information according to precedence, with

mission-critical messages such as medevac requests or calls for fire receiving higher priority. Vital information is delivered ahead of routine data.

The Army began fielding the first increment of WIN-T in 2004 to support operations in Iraq and Afghanistan. WIN-T Increment 2 is currently being fielded and deployed as the mobile network backbone of Capability Set 13. The advanced integrated, interoperable communications capabilities of CS13 provide connectivity across the entire BCT formation from the stationary Command Post to the commander on-the-move all the way down to the dismounted Soldier. WIN-T Increment 2 is the mobile tactical communications network backbone of the capability set, equipping Soldiers with high-speed, high-capacity voice, data and video communications down to the company level.

The ability of WIN-T NetOps to help retain strong network connections even in difficult terrain is aiding the Army in its advise-and-assist operations in Afghanistan. The 4th BCT, 10th Mountain Division (Light Infantry), which deployed to Afghanistan this past summer, is the first unit to utilize CS13 in theater, and 3/10 joined them in the fall. The 101st Airborne Division Headquarters also uses WIN-T Increment 2 elements

in that theater. Meanwhile, the 2nd and 3rd BCTs of the 101st Airborne Division are undergoing CS13/WIN-T Increment 2 fielding and training operations.

With the increased capabilities provided by CS 13 now in theater and the Army beginning deliveries of follow-on capability sets, the basic principles of the communication officer's job will remain the same, but what will change is the complexity and density of equipment. The Army has merged radio and satellite networks all the way down to a platoon and sometimes even squad level with Internet Protocol-based communications, which it hasn't used before at those echelons. That complexity requires more systems and more efficiency in NetOps. A singular piece of equipment will no longer stand on its own, Tornabell said.

"If a system functions great on its own that's good, but once it's integrated into a network it can affect a different piece of equipment completely outside the scope of that operator and unit; it can have an impact all the way up to the corps level depending on information dissemination policies," he said. "The WIN-T NetOps tools help provide us with better situational understanding across the entire network."

(Continued on page 36)

(Continued from page 35)

In the past, Army programs developed their own stove-piped NetOps solutions for their own particular systems and domains. But the Army is now looking at NetOps from a more holistic, simplified standpoint and efforts are underway to provide an integrated set of tools that allow the S6 to “fight” each system across the various domains, echelons, and transport and computing infrastructures resident in tactical formations.

In 2012 Heidi Shyu, the Army Acquisition Executive, designated the Program Executive Office for Command, Control, and Communications-Tactical, to which PM WIN-T is assigned, as the lead for Integrated Tactical NetOps. In this role, the organization is synchronizing efforts across the Army to integrate and converge NetOps capabilities. The goal is to achieve network visibility from the enterprise level to the tactical level, while reducing the number of tools required. Integrating NetOps, from the enterprise to the tactical edge, will achieve efficiencies and improve operational flexibility.

An improved WIN-T NetOps suite developed under the WIN-T Increment 3 program will serve as the baseline for tactical NetOps as the Integrated Tactical NetOps team works to converge

other products, such as those used to manage the lower tactical internet. An early success for lower TI NetOps convergence was realized with the fielding CS(13)’s Joint Tactical Networking Environment NetOps Toolkit, which collapsed several lower tactical network tools, mostly radio management tools, onto one laptop, helping to streamline how the S6 manages the tactical network.

This spring the next version of the advanced WIN-T NetOps capabilities are scheduled to be further evaluated at NIE 14.2, before they are eventually fielded to WIN-T Increment 2 units as a quarterly release update. Looking forward, as new technologies are developed, standard WIN-T NetOps tools will be inherent in a product’s initial design instead having to be collapsed after the product has already been

fielded.

“NetOps convergence is a journey,” said Lt. Col. Ward Roberts, product manager for WIN-T Increment 3, who is leading the Integrated Tactical NetOps team. “Our goal at the end of the day is to make the S6’s job as easy as possible by ensuring he has an integrated set of tools to initialize, operate and fight that system as part of an advanced, integrated network.”

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

ACRONYM QuickScan

2/1 AD - 2nd Brigade, 1st Armored Division

3/10 - 3rd Brigade Combat Team, 10th Mountain Division (Light Infantry)

BCT - Brigade Combat Team

CS - Capability Set

J-TNT - Joint Tactical Networking Environment NetOps Toolkit

NetOps - Network Operations

NIE - Network Integration Evaluation

PEO C3T - Program Executive Office for Command, Control, and Communications-Tactical

S6 - Communications Officer (S6)

TI - Tactical Internet

WIN-T - Warfighter Information Network-Tactical

A common services dictionary

By Robert Dillow and Sam Edelman

The consensus is that Network Operations services need to be standardized across the Army. Standardization across the spectrum is a colossal task but begins by agreeing on the definitions for the services that compose NetOps.

How hard can that be?

Remember the old military joke about securing a building? If you give the command “Secure the building,” the Navy would turn out the lights and lock the doors; the Army would surround the building with defensive fortifications, tanks and concertina wire; the Marine Corps would assault the building, using overlapping fields of fire from all appropriate points on the perimeter; and the Air Force would take out a three-year lease with an option to buy the building.

Just like the joke, the NetOps Communities of Interest (governance, tactical operational, strategic operational and acquisition) often had different definitions for the same NetOps services. This led to too many disparate NetOps services, functions and capability

lists that caused confusion across the NetOps community. The programmatic community also found it difficult to identify solutions that perform similar or identical service functions when performing system/portfolio reviews.

The Gartner Chart of Information Technology’s growing transparencies and Significant Enterprise Impacts below illustrates how broad the IT world of services and capabilities has become, see.

To support the NetOps environment community, a task force of NetOps stakeholders led by the Army CIO/G-6 recently defined services for the NetOps Trail Boss in four priority areas: Security Supporting Infrastructure Defense, Information Technology Asset Management, Service Management, and Spectrum Management Operations.

The NetOps task force supporting the NetOps Trail Boss under the Program Executive Officer for Command, Control Communications Tactical included representatives from: PEO C3T, U. S. Cyber Command, PEO for Enterprise Information Systems, TRADOC Capability Manager for Global Network Enterprise, Network Enterprise Technology Command, Chief Information Officer/G-6, Army Signal Center of Excellence, Program Manager Mission Command, U.S. Army Cyber Command, Training and Doctrine Command Architecture Integration and Management Directorate, and Assistant Secretary of the Army (Acquisition, Logistics and Technology) or ASA(ALT).

The team aligned its work to DoD and Joint references and developed a thesaurus that evolved into a common dictionary of NetOps services. This authoritative list of IT services is closely aligned to the DoD Information Enterprise Architecture service descriptions

Gartner Top End-User Predicts 2011—Analysis:

- By 2015, tools and automation will eliminate 25% of labor hours associated with IT services.
- By 2015, most external assessments of enterprise value and viability will include explicit analysis of IT assets and capabilities.

Two of IT’s growing transparencies

(Continued on page 38)

(Continued from page 37)

with some modifications.

In some areas the Army added services that support the Army NetOps Architecture Operational Viewpoint not covered within DIEA. Some definitions were modified for clarity or specialized to meet Army requirements. The NetOps IT services were grouped to align to the DIEA categories since most Army organizations have traditionally grouped NetOps services according to the older constructs.

Doctrinally some Spectrum Management Operations reside outside traditional NetOps activities; however, spectrum management is a key enabler of successful network operations. Because NetOps cannot function without spectrum management in the tactical arena, Spectrum Management Operations services are placed within the NetOps service area.

This collaborative effort produced a comprehensive NetOps Services Integrated Dictionary (AV-2). This AV-2 document represents agreement among all stakeholders and is a single source of standardized NetOps services and their corresponding definitions. The NetOps Services Integrated Dictionary is available on the Army Capability Architecture Development and Integration Environment site at: <http://go.usa.gov/KDXY> (CAC required).

The NetOps Architecture Services Integrated Dictionary is now the AV-2 for the Army NetOps Technical Reference Architecture and is a companion to TRADOC's Army NetOps Architecture Operational and the Assistant Secretary of the Army for Acquisitions, Logistics, and Technology's Army Network Operations integrated System Engineering Plan.

This NetOps Services Integrated Dictionary also meets some parallel needs. It will be used in the Network Management Area of Army IT Management Reform, Army IT portfolio management for budget reviews, and the pending development of a consolidated NetOps Concept of Operations that encompasses the entire LandWarNet design.

The results of this effort are in line with the Army leadership's direction to build a network that connects our forces at all echelons. This AV-2 is an authoritative

source of services for Army program managers to align their programs; it also assists in eliminating duplicative services in the Army inventory and increases collaboration, communication, and understanding among Army users.

Sam Edelman has 36 years of experience managing information technology and telecommunications organizations, systems, programs, projects, and acquisitions from the tactical through the operational to the strategic level through all phases of their life cycles. He is a Femme Comp Inc. senior systems analyst working for the Army's Chief Information Officer G-6's Army Architecture Integration Center. He is a graduate of Appalachian State University, in North Carolina with a Bachelor of Science degree in broadcasting. His military education includes: Signal, Logistics, Satellite, Mobile Subscriber Equipment.

Bob Dillow is responsible for leading Serco Department of Defense, Commercial and Civilian programs within Headquarters (HQ) U.S. Army (G6), HQ Air Force Space Command, and the Boeing Company. He is a retired U.S. Air Force master sergeant with over 30 years of experience in the intelligence and space communities. He possesses a Master's degree in computer resource information management from Webster University. He is a certified information systems security professional and holds the information technology

Gartner: Top 10 Strategic Technology Trends for 2014.

Gartner just concluded its Gartner Symposium/ITxpo, 6-10 Oct, 2013 in Orlando with tens of thousands of IT Executives and are the Gartner IT predictions:

1. Mobile Device Diversity and Management
2. Mobile Apps and Applications
3. The Internet of Everything
4. Hybrid Cloud and IT as Service Broker
5. Cloud/Client Architecture
6. The Era of Personal Cloud
7. Software Defined Anything
8. Web-Scale IT
9. Smart Machines
10. 3-D Printing

Significant Enterprise Impacts

infrastructure library foundations certification. His Enterprise Architect team is a two-time

winner of the Boeing Supplier of the Year award and the recipient of the 2010 Department of

Defense Enterprise Architecture Achievement Award—Industry category.

ACRONYM QuickScan

AIMD - Architecture Integration and Management Directorate
AV - All Viewpoint
ArCADIE - Army Capability Architecture Development and Integration Environment
ARCYBER - US Army Cyber Command
ASA (ALT) - Assistant Secretary of the Army for Acquisitions Logistics & Technology
CIO - Chief Information Officer
DIEA - DoD Information Enterprise Architecture
DoD - Department of Defense
HQ - Headquarters
IT - Information Technology

ITAM - Information Technology Asset Management
NETCOM - Network Enterprise Technology Command
NetOps - Network Operations
PEO C3T - Program Executive Office for Command, Control Communications Tactical
PEO EIS - Program Executive Office for Enterprise Information Systems
TCM GNE - TRADOC Capability Manager for Global Network Enterprise
ToR - Terms of Reference
TRADOC - Training and Doctrine Command
USCYBERCOM - U. S. Cyber Command

Army Communicator is authorized Periodical Mailing Privileges by the U.S. Postal Service and is required to publish a completed Statement of Ownership, Management and Circulation each year. This report includes all pertinent information for all issues of the publication in which the statement is printed.

UNITED STATES POSTAL SERVICE® (All Periodicals Publications Except Requester Publications)

1. Publication Title: **ARMY COMMUNICATOR**

2. Publication Number: **3 0 5 1 4 7 0**

3. Filing Date: **1 DEC 2013**

4. Issue Frequency: **QUARTERLY**

5. Number of Issues Published Annually: **FOUR (4)**

6. Annual Subscription Price: **\$0**

7. Complete Mailing Address of Known Office of Publication (Not printer) (Street, city, county, state, and ZIP+4®):
U.S. ARMY SIGNAL CENTER OF EXCELLENCE, 513 CHAMBERLAIN AVE. BLDG 29808A RM 713, FT. GORDON, (RICHMOND CTY), GA 30905-5301

Contact Person: **LARRY EDMOND**

8. Complete Mailing Address of Headquarters or General Business Office of Publisher (Not printer):
CHIEF OF SIGNAL, U.S. ARMY SIGNAL CENTER OF EXCELLENCE, 513 CHAMBERLAIN AVE. BLDG 29808A FT. GORDON, (RICHMOND CTY), GA 30905-5301

9. Full Names and Complete Mailing Addresses of Publisher, Editor, and Managing Editor (Do not leave blank):
Publisher (Name and complete mailing address):
CRAG ZIMMERMAN, OCCAS DIRECTOR, U.S. ARMY SIGNAL CENTER OF EXCELLENCE, 513 CHAMBERLAIN AVE. BLDG 29808A, FT. GORDON, (RICHMOND CTY), GA 30905-5301
Editor (Name and complete mailing address):
LARRY EDMOND, U.S. ARMY SIGNAL CENTER OF EXCELLENCE, 513 CHAMBERLAIN AVE. BLDG 29808A RM 713, FT. GORDON, (RICHMOND CTY), GA 30905-5301
Managing Editor (Name and complete mailing address):
NONE

10. Owner (Do not leave blank. If the publication is owned by a corporation, give the name and address of the corporation immediately followed by the names and addresses of all stockholders owning or holding 1 percent or more of the total amount of stock. If not owned by a corporation, give the names and addresses of the individual owners. If owned by a partnership or other unincorporated firm, give its name and address as well as those of each individual owner. If the publication is published by a nonprofit organization, give its name and address.)

Full Name	Complete Mailing Address
U.S. DEPT OF THE ARMY	105 ARMY PENTAGON, WASHINGTON, DC 20310-0105

11. Known Bondholders, Mortgagees, and Other Security Holders Owning or Holding 1 Percent or More of Total Amount of Bonds, Mortgages, or Other Securities. If none, check box None

Full Name	Complete Mailing Address
-----------	--------------------------

12. Tax Status (For completion by nonprofit organizations authorized to mail at nonprofit rates) (Check one)
The purpose, function, and nonprofit status of this organization and the exempt status for federal income tax purposes:
 Has Not Changed During Preceding 12 Months
 Has Changed During Preceding 12 Months (Publisher must submit explanation of change with this statement)

PS Form 3526, September 2007 (Page 1 of 3 (Instructions Page 3)) PSN 7530-01-000-9931 PRIVACY NOTICE See our privacy policy on www.usps.com

ARMY COMMUNICATOR FALL December 2013

15. Extent and Nature of Circulation	Average No. Copies Each Issue During Preceding 12 Months	No. Copies of Single Issue Published Nearest to Filing Date
U.S. ARMED FORCES-CONUS		
a. Total Number of Copies (Net press run)	6,500	6,500
(1) Mailed Outside-County Paid Subscriptions Stated on PS Form 3541 (includes paid distribution above nominal rate, advertiser's proof copies, and exchange copies)	NONE	NONE
(2) Mailed In-County Paid Subscriptions Stated on PS Form 3541 (includes paid distribution above nominal rate, advertiser's proof copies, and exchange copies)	NONE	NONE
(3) Paid Distribution Outside the Mails Including Sales Through Dealers and Carriers, Street Vendors, Counter Sales, and Other Paid Distribution Outside USPS®	NONE	NONE
(4) Paid Distribution by Other Classes of Mail Through the USPS (e.g. First-Class Mail®)	5,571	5,571
c. Total Paid Distribution (Sum of 15b (1), (2), (3), and (4))	5,571	5,571
(1) Free or Nominal Rate Outside-County Copies included on PS Form 3541	100	100
(2) Free or Nominal Rate In-County Copies included on PS Form 3541	50	50
(3) Free or Nominal Rate Copies Mailed at Other Classes Through the USPS (e.g. First-Class Mail)	10	10
(4) Free or Nominal Rate Distribution Outside the Mail (Carriers or other means)	300	300
e. Total Free or Nominal Rate Distribution (Sum of 15d (1), (2), (3) and (4))	460	460
f. Total Distribution (Sum of 15c and 15e)	6,031	6,031
g. Copies not Distributed (See Instructions to Publishers #4 (page #3))	469	469
h. Total (Sum of 15f and g)	6,500	6,500
i. Percent Paid (15c divided by 15f times 100)	85.7%	85.7%

16. Publication of Statement of Ownership
 If the publication is a general publication, publication of this statement is required. Will be printed in the **Winter 2013** issue of this publication.
 Publication not required.

17. Signature and Title of Editor, Publisher, Business Manager, or Owner
Larry Edmond
LARRY EDMOND, EDITOR-IN-CHIEF
Date: **5 DEC 2013**

I certify that all information furnished on this form is true and complete. I understand that anyone who furnishes false or misleading information on this form or who omits material or information requested on the form may be subject to criminal sanctions (including fines and imprisonment) and/or civil sanctions (including civil penalties).

PS Form 3526, September 2007 (Page 2 of 3)

Think. Write. Publish.

By MAJ Joe Byerly

Junior to mid-grade leaders, both officers and NCOs, do a lot of thinking!

These leaders constantly develop innovative solutions for problems, ranging from the simple to extremely complex, during combat deployments, training exercises, and garrison activities.

These solutions or ideas are worth hearing about, however many of these young leaders remain professionally silent.

Published articles by this demographic of Army leaders are extremely important to their personal development and to our profession, but are also extremely rare.

It's not that these leaders necessarily have better ideas than the command sergeants major, colonels, or general officers. It's simply that they bring a fresh outlook to the

"Nail your whispers to the wall. Conclude the trilogy of read..think..and write. Is there 'career risk' in publishing? I suppose. Hasn't hurt me too badly over the years, I'd say. But what matters is testing your ideas on the field of intellectual battle, so to speak."

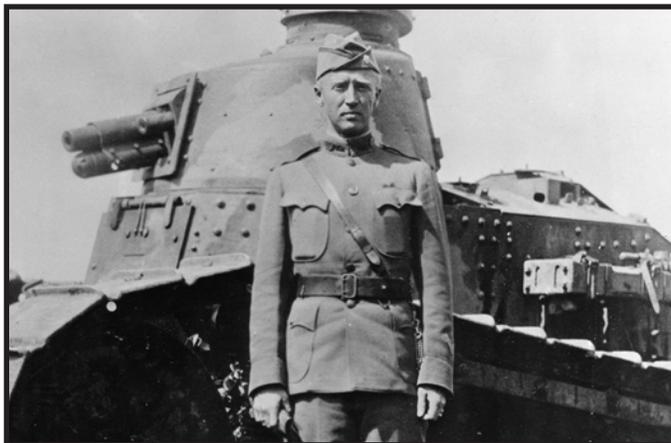
professional discourse that takes place in our military journals and other outlets.

To further illustrate this point, think about when you PCS.

If you're anything like me, after living in a new house for only a month, I no longer notice those things that bothered me when I first moved in. It usually takes someone who doesn't live with me, to bring them back to my attention. Similarly, NCOs and officers that have been in

the service for a decade or more may have become blind to those blemishes and annoyances that still are fresh in the eyes of younger leaders. It is this voice we need to continue to hear through publication in printed journals and online blogs. A desire by younger men and women in the Army to improve themselves, and in the process their craft, is nothing new. Take for example two innovative officers in the Interwar Period. In the fall of 1919, MAJ Dwight Eisenhower and LTC George Patton began spending a considerable amount of time training, experimenting, and discussing new methods of tank warfare at Camp Meade. They saw the possibility of using tanks to achieve rapid breakthroughs vice just moving in support of the infantry. MAJ Eisenhower captured these ideas in writing and published them in a 1920

LTC George S. Patton, 1st Tank Battalion, with a French Renault Tank, Summer 1918.



Infantry Journal article, titled "A Tank Discussion." The article wasn't well received because it ran counter to the accepted doctrine. Eisenhower was reprimanded by the Chief of Infantry, MG Charles S. Farnsworth, who told him that his ideas were dangerous, and that if he tried to publish them again he would face a court-martial.

At the time of publication, MAJ Eisenhower had only five years of experience and the tank was still a nascent technology on the battlefield. He wasn't overly invested in the tactical doctrine, so his creativity wasn't stifled. He faced some pressure for publishing his thoughts, but in the end it contributed to a professional discussion that eventually led to better doctrine for the inclusion of armor in the fight.

Today's younger officers and NCOs have more battlefield experience, and more practice at creating innovative solutions to combat situations, than most recent generations. Unfortunately, their new perspectives and ways of doing business are largely kept at the unit level or shared among groups of friends. They are thinking, and hopefully writing, but too few are publishing.

This is something that we must change. In the words of ADM (R) Jim Stravridis, "publishing your thoughts for others to see.... extends the reach of your ideas and sparks a larger discussion, a larger professional conversation." Following a decade of



GEN Dwight D. Eisenhower

lessons learned in and out of combat, we need this larger conversation to occur so that the profession may continue to evolve and adapt.

A few years ago, I decided to move beyond thinking into writing and publishing. In 2011, I came out of my second command and, for the first time in eight years, had a considerable amount of time for reflection. I whipped out a green notebook and began to write, and write, and write some more.

While this was great for me personally, it wasn't that valuable to the profession. After reading the blogs and articles from current leaders like Jonathan Silk, Nathan Finney, and Benjamin Kohlmann, I decided to compile my notebook scribbles into substance for publication. One of the first articles I wrote took me 4 months, numerous drafts, and constant sharing with friends and mentors for comments. I remember being excited and anxious as I finally

submitted it for publication to Military Review. It only took a few weeks to receive a rejection notice.

While I was disappointed, I had an idea that was no longer simply in my head, it had crystallized in written form. I passed it around and a couple of things happened.

First, I was offered a temporary assignment to work on a project that was related to my article. I got to see a concept that I wrote about come to life, thus giving me a chance to affect the greater profession.

Second, a higher-ranking officer reached out to me and combined pieces of my rejected article with his research to produce a piece that was published in the May-June 2013 issue of Military Review.

Those events validated for me the point that if junior leaders want to affect change, make the profession better, or just share experiences with others, we need to step onto the battlefield of ideas with our thoughts captured in writing.

In the process of publishing, and from lessons gleaned from the reading of history, here are some lessons I learned.

1. Multiple drafts/Multiple sets of eyes

None of my articles/posts have ever been ready for publication after the first, second, or even the third draft. There are always grammatical errors or structural problems that I might miss, so I pass it

(Continued on page 42)

along to a friend for review. After finalizing the edits, I may pass it on to one more person for a final look. One more set of eyes never hurts.

2. Seek out mentors to develop articles

In addition to potentially coauthoring articles, mentors can provide additional insight, offer a more seasoned perspective, and provide additional resources to bolster the article

3. Be prepared for feedback

To paraphrase Stravridis, publishing articles is like nailing your whispers to the wall for everyone to see. Not everyone is going to agree with your viewpoints, but that is okay. Negative feedback is nerve-racking and scary; however it lets you know that people are at least reading your efforts. Hearing from or reading comments from others who disagree with your viewpoints offers you the opportunity to see differing outlooks on the subject, which may help to deepen your understanding of the subject you wrote about.

4. Writing closes doors

Many published leaders have had doors close on them throughout their careers when they brought ideas, especially those that ran counter to the collective thought, to the battlefield of

Bronze created for MacArthur Memorial Foundation. The author was presented one of these busts as a 2011 MacArthur Leadership Award recipient.



ideas. Something to keep in mind is that while writing can close doors, it can also open doors.

5. Writing opens doors

MAJ Eisenhower's article in Infantry Journal may have closed some doors within the Infantry Branch, but it also may have served as a building block in his relationship with Fox Conner. One of Conner's own articles, published 10 years earlier, "Field Artillery in Cooperation with Other Arms," led to revisions in artillery doctrine. Without Fox Connor's mentorship of Eisenhower, much of the military history of the mid-twentieth century would be quite different. As in the past, today there are senior leaders in the Army that will champion initiatives...but they need to read about them first.

6. There's a venue for everyone

From online military blogs like Small Wars Journal and War on the Rocks, to branch magazines like Armor and Infantry Magazine, there is a venue for every leader at every level. Chances are there is at least one that would be interested in your (well-written) idea.

In less than a week, I will take the next step in my professional career, moving from company grade to field grade officer. While I hope that my views will always remain current and relevant, I know that over time I may become blind to those things that can and should be changed.

One way to avoid this blindness is to continue to read published articles of company grade officers and NCOs, as well as working with those interested in writing. The next crop of Pattons and Eisenhowers are currently walking among us, and I would love to read their thoughts.

Joe Byerly has served as a Cavalry platoon leader in a Stryker Brigade Combat Team and a troop and headquarters company commander in an Armored Brigade Combat Team. He currently serves as an instructor at the School of Reconnaissance and Security. He was a 2011 recipient of the GEN Douglas MacArthur Leadership Award.

Join the Discussion

<https://SIGKN.army.mil>



Publish your articles in the

ARMY COMMUNICATOR

A task that should be on the radar of every Soldier is publishing an article in the Army Communicator, the U.S. Army Signal Regiment's professional magazine. The journal explores trends in the Regiment and provides a place for Signal Regiment members to share good ideas and lessons learned with your colleagues.

The Army Communicator publishes quarterly and depends on noncommissioned officers, officers, warrant officers and Regimental civilian employees to contribute quality articles on topics of interest to the entire Regiment.

Not only does the Army Communicator provide a great resource for professional development but it also offers an excellent platform for new authors to break the ice in submitting their first manuscript for publication. It helps your fellow service members to gain insights from your experiences and bodes well when you can lay claim to publication in an internationally recognized and well-respected professional journal.

Nothing Ventured, Nothing Gained

Some are plagued by a lack of confidence and fear of having an article rejected. For others, it is lack of knowledge about the writing style or how the publishing process works. Copies of the Army Communicator, Guidelines for Writing and Submitting manuscripts and the acceptable style can be found on-line at:

<http://www.signal.army.mil/OCOS/AC/>

Peruse the site and submit an article. There are numerous opportunities, book reviews, letters to the editor, lessons learned, future trends, awards and commendations, how-to, etc.

The good news is that when you submit an article it can be accepted, pending some revisions. The worst that can happen is that it will be rejected, but as part of that process, you will most likely receive invaluable, constructive comments on how your research and/or write-up can be improved. You will then be at liberty to submit the revised manuscript.

The end result will be a win-win for the Regiment and for you.

Letter to the Editor

Feedback



Editor,

I believe we can strengthen our cyber leadership posture through strategic Mission Command assignments.

Technology and the digital environment have introduced and influenced one of the most dynamic and asymmetric battlefields of the 21st Century. The World Wide Web presents an increased threat of what is referred to as “cyber-based attacks.” The ever expanding Department of Defense digital resources, with over 15,000 computer networks across 4,000 military bases in 88 countries, has increased vulnerabilities and led to concerns over the segregation of these resources across the Department of Defense and the sister Services.

The ever growing joint and inter-agency operational environment, in conjunction with the increased necessity to trust sister organizations, will begin to mold the cyber warrior and shift the dynamics of how the Armed Forces train future Soldiers, Sailors, Airmen, and Marines. General Dempsey emphasized that “Mission Command for Joint Force 2020 requires trust at every echelon of the force.”

As the U.S. Government continues to define and function in the complex operating environment of cyberspace, commanders and leaders at all levels must develop dynamic, malleable, and knowledgeable leaders, as well as soldiers, to combat the emerging cyber threats. Commanders will need to establish learning environments and opportunities that allow for discipline initiative, while accepting there will be the occasional failures. In return, leaders must establish a culture and climate within the organization that fosters prudent risk, while ensuring failure is survivable – a safe fail. Lastly, commanders and organizations must learn from their failures. Often, leaders and organizations observe lessons, though fail to inculcate them into the organization’s culture to truly learn from their failures.

While a cyber warrior must be technically and tactically proficient in the cyber domain, it is just as critical that he/she be a better leader in the asymmetric dynamics of cyberspace. The demands of cyberspace, evolution, progression, and continued ambiguity of the environment requires leaders who are agile, adaptive, and aggressive.

There is a direct correlation between Mission Command and the development of current and future cyber warriors throughout all formations, organizations, and agencies within the United States. While a single agency cannot protect and defend cyberspace alone, the government and private sector, collectively, can effectively defend the nation’s assets.

The Army must take prudent risk in the placement of its leaders within key cyber organizations. While maximizing a leader’s expertise – right person for the right job at the right time – is critical to ensuring effective organizations, broadening is essential for leader development, as well as the propagation of the expert’s knowledge to the rest of the force.

MAJ Clifford M. Woodburn



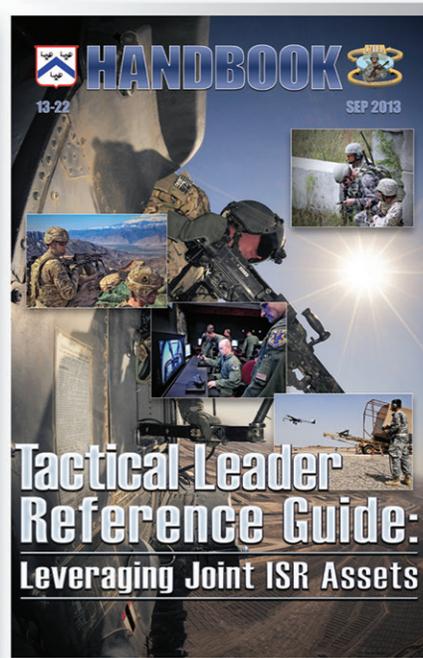
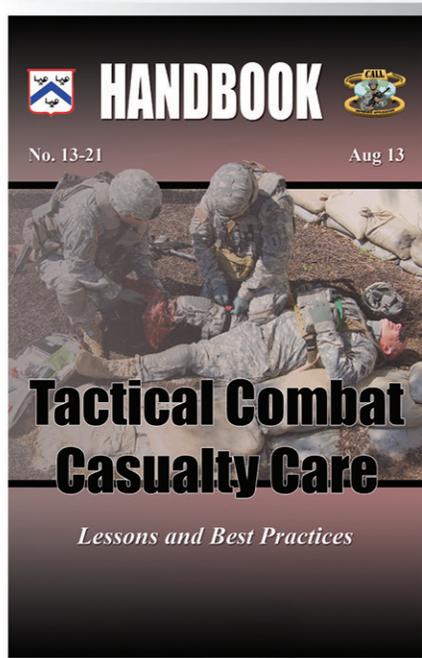
Center for Army Lessons Learned

10 Meade Avenue, Building 50, Fort Leavenworth, KS 66027

COM: (913) 684-9533

DSN: 552-9533

Check out our latest publications.



Visit the CALL Website for more publications.

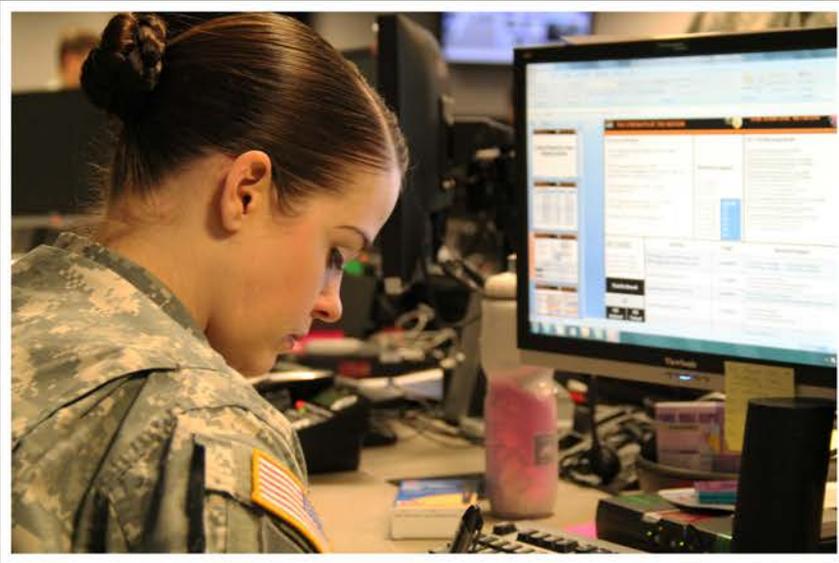
Public Website:
<http://call.army.mil>

**Restricted Website
(CAC access):**
<https://call2.army.mil>

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

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

OFFICIAL BUSINESS
ISSN 0362-5745



The Signal Regiment is at the forefront of the country's ongoing mission to dominate cyberspace. The next issue of the Army Communicator offers a state-of-the-force look at the newest military occupational specialty - 25D, Cyber Network Defender and some sweeping changes coming as the Signal Center of Excellence morphs into a Signal/Cyber training center.



Signal Towers, Room 713
Fort Gordon, Georgia 30905-5301
PIN: 104136-000