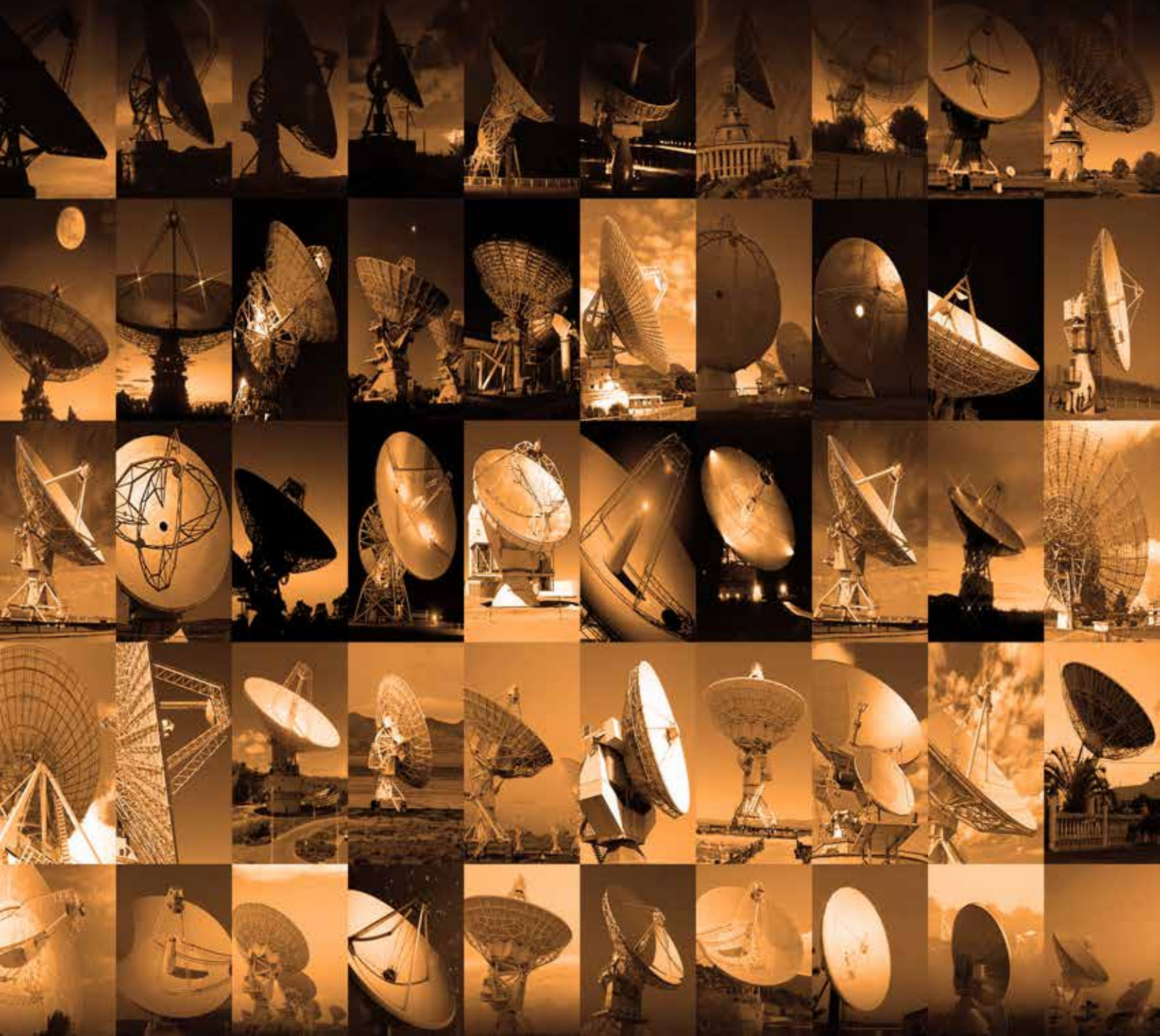
# ARMY COMMUNICATOR

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

PB 11-14-3 2014 Vol. 39 No. 3

# The Signal Regiment



# SIGNAL CORPS FOREVER

The Signal Corps is one of the first combat support branches to become organized under the U. S. Army Regimental System. The purpose of the regimental system is "to enhance combat effectiveness through a framework that provides the opportunity for affiliation, develops loyalty and commitment, fosters a sense of belonging, improves unit esprit, and institutionalizes the war-fighting ethos."

On June 1, 1986, the Signal Corps (Regiment) was formed under the whole branch regimental concept.

Under the whole branch regimental concept, all Signal Soldiers are affiliated with the Signal Corps in a lifelong relationship. This means that as a Signal Soldier, no matter where you are assigned or how often you move, your professional home will always be Fort Gordon, and your regiment will always be the Signal Corps.

U.S. Army Signal School
fort gordon

## Command

**Chief of Signal**
COL Thomas A. Pugh

**Regimental Chief Warrant Officer**
CW5 Peter T. Winter

**Regimental Command Sergeant Major**
SGM Valerie Green

## Editorial Staff

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

**Art Director/Graphic Designer**
Billy Cheney

**Photography**
Billy Cheney, Bill Bengston, Amy Walker, Lawrence Holgate, CPT Jeff Stevens, SGT Erneston Gonzales

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

GERALD B. O'KEEFE
*Administrative Assistant to the Secretary of the Army*
Authorization 1428701

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

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

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

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

***Army Communicator*** reserves the right to edit material.

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

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

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

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

**PB 11-14-03**
**Winter 2014**
**Vol. 39 No. 3**

# Army Communicator

## *Voice of the Signal Regiment*

### Table of Contents

*Features*

4 **New commander leads Cyber Center of Excellence**
Kimberly Lewis

6 **Outlining the vision**
MG Stephen G. Fogarty

8 **Colorless core improves network interoperability**
Amy Walker

12 **National Security Agency's Host Mitigation Initiative**
MAJ Paul Meaux
Kevin Corbitt

16 **Signal officers leveraging Lean Six Sigma**
CPT Asheesh Nikore

18 **Gunslingers complete mission**
CPT Thomas A. Allen

19 **198th ESB closes technical control facility**
CPT Jeff Stevens

22 **Technical control facility in a box offers benefits**
SPC Derek W. Kinhofer

24 **High capacity line of sight solutions**
CW2 Angel Gonzales

27 **298th Signal Company dedicates new enterprise terminal**
1LT Genevieve Jarrett

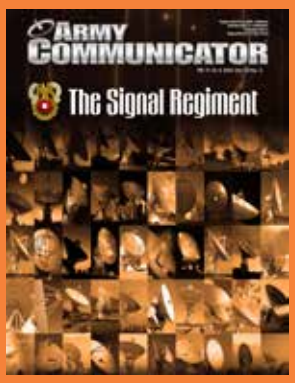
28 **It's time to get ready for cyber warfare**
LTC Frank Beyer

36 **Reclassified MOS 25F Soldiers negotiating new training requirements**

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

*~On the Cover~*
## Ground Satellite Installations

*Even as the communications landscape continues to change at the speed of light, there are some iconic images that serve to remind us that the foundational services provided by Signal Regiment professionals continue to be an integral part of all operations.*




*Cover design by Billy Cheney*

# Fulfilling the Signal Corps Mission

On April 1, 1920, the Office of the Chief Signal Officer announced and published the first "bimonthly bulletin of information" designed to provide Signal Corps officers an information sharing platform.

***Since 1920, the Army Communicator has kept Signal Regiment members interested in our branch of service and the profession of arms.***

The spirit of this original information bulletin exists today in the Army Communicator. There have been changes over the years. The Army Communicator is now a quarterly periodical that provides all members of the Signal Regiment--officer, enlisted and civilian--a medium to share professional information.

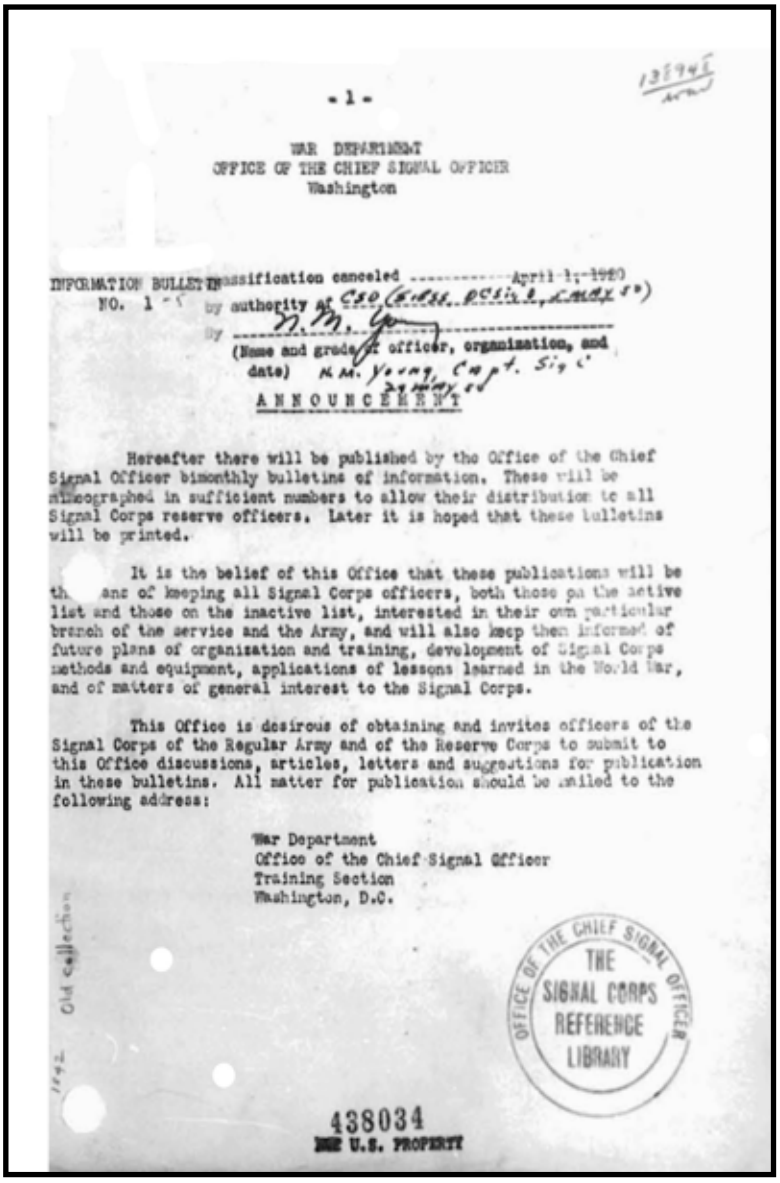
Over the past 95 years, the original purpose of the information bulletin has not changed. Its purpose was to keep members of the Signal Corps "Interested in their own particular branch of service and the Army, and will also keep them informed of future plans of organization and training, development of Signal Corps methods and equipment, applications of lessons learned…, and of matters of general interest to the Signal Corps."

As with the original information bulletin, the success of the Army Communicator depends on you. Its success depends on your input of "discussions, articles [and] letters." Its success depends on your suggestions for topics and improvements. Its success depends on your sharing the articles and information with those who have not seen or read them before. Most importantly, its success depends on your consumption of the information contained within these pages and importing the knowledge to others.

Pro Patria Vigilans!

Join the Discussion

https://SIGKN.army.mil



- 1 -

WAR DEPARTMENT
OFFICE OF THE CHIEF SIGNAL OFFICER
Washington

INFORMATION BULLETIN Classification canceled ---------- April 1, 1920
NO. 1 by authority of CSO (Cir. 85, C.S.O. 1, Cmdr 8)
By M. M. Young
(Name and grade of officer, organization, and date) M. M. Young, Capt. Sig C

ANNOUNCEMENT

Hereafter there will be published by the Office of the Chief Signal Officer bimonthly bulletins of information. These will be mimeographed in sufficient numbers to allow their distribution to all Signal Corps reserve officers. Later it is hoped that these bulletins will be printed.

It is the belief of this Office that these publications will be th ans of keeping all Signal Corps officers, both those on the active list and those on the inactive list, interested in their own particular branch of the service and the Army, and will also keep them informed of future plans of organization and training, development of Signal Corps methods and equipment, applications of lessons learned in the World War, and of matters of general interest to the Signal Corps.

This Office is desirous of obtaining and invites officers of the Signal Corps of the Regular Army and of the Reserve Corps to submit to this Office discussions, articles, letters and suggestions for publication in these bulletins. All matter for publication should be mailed to the following address:

War Department
Office of the Chief Signal Officer
Training Section
Washington, D.C.

OFFICE OF THE CHIEF SIGNAL OFFICER
THE SIGNAL CORPS REFERENCE LIBRARY
438034
U.S. PROPERTY

**Above is a copy of the cover letter dated 1920 from the Office of the Chief of Signal for the first information journal that has evolved into the Army Communicator you are now reading. In the coming months, we will continue sharing historical information that illustrates the exceptional legacy of the Signal Regiment and the reasons you should take great pride in your Signal Corps.**

# Signal Regiment more relevant than ever

Signaleers,

Today's Army Signal Corps comprises the force that builds, maintains, operates, defends and secures all of the networks to meet the needs of our expeditionary land forces.

In the foreseeable future, we will continue to be a vital part of the fight; providing tactical and strategic communications platforms for our direct action and support units.

To maintain our relevant position in the years ahead, we must grow our internal capabilities, learn to leverage commercial networks, and explore ways to better disseminate intelligence to the lowest level all while staying on the cutting edge of technology and training.

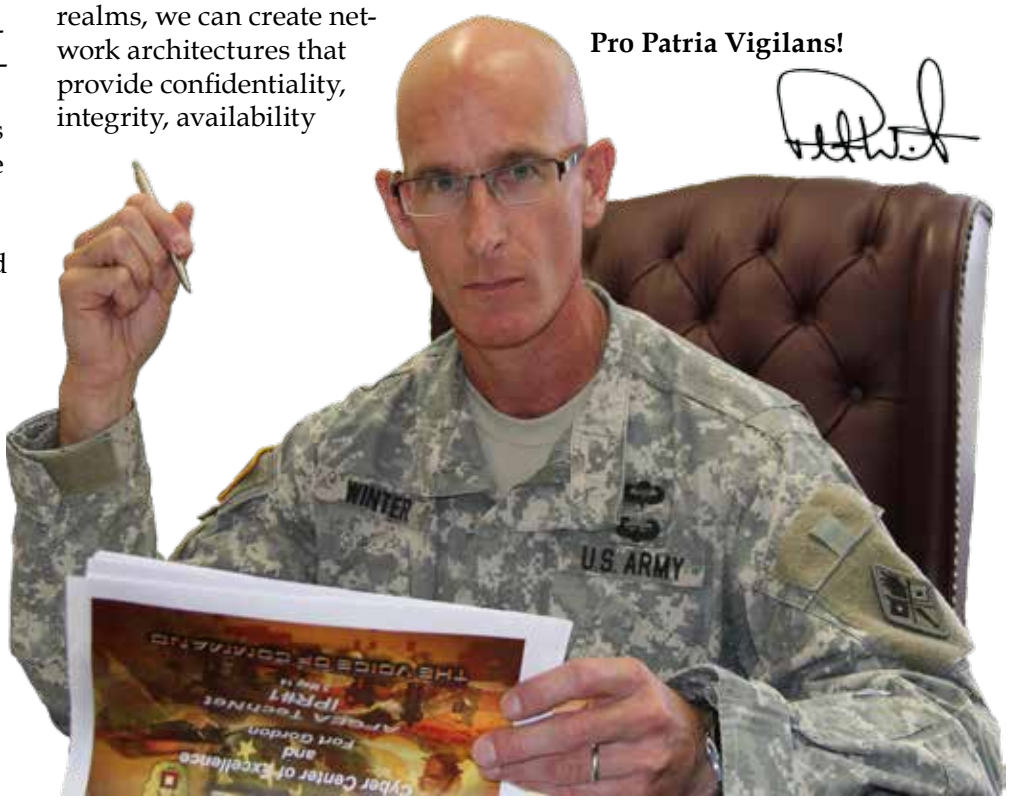
As new capabilities are developed, we must ensure we can quickly acquire new technology and smoothly integrate it with the systems fielded to our units. All Signaleers must keep closely connected to the Signal schoolhouse through constantly changing on-demand, live and virtual constructive integrated training. As budget cuts result in a more streamlined field service representatives support force, our own Signaleers must develop expert troubleshooting and maintenance skill sets. The end result will be a Signal force that is increasingly self-reliant.

Another area for growth is the exploration of integrated networks. Whether leveraging organic host nation networks, or tapping into our own commercial assets, we must continue providing robust communications and capabilities at all phases of military operations. Army forces must be networked, linked and synchronized in order to enable more efficiency as dispersed forces attempt to communicate, maneuver, share information and collaborate through a common operating picture. Enabling quick reaction forces with actionable intelligence and full motion video immediately prior to an operation increases the odds for success.

The necessity for security and reliability on our networks makes it necessary to work hand-in-hand seamlessly with our cyber peers to mitigate risks and threats in our networks. In fact, cyberspace protection and communications network development are inextricably linked. By anticipating the challenges in both realms, we can create network architectures that provide confidentiality, integrity, availability and security while enabling us to draw on existing network infrastructure.

Critical to meeting the challenges before us are our functional area and warrant officer experts. With an eye on the strategic picture, the Signal Corps will rely on you to think outside the box, developing tactically sound but operationally creative solutions that will enable our Army to leverage and integrate emerging technologies. As we have no idea what the future may hold, we must prepare ourselves to meet any contingency, less dependent upon outside support. With rapidly-evolving battlefields, we must seek out ways to our Armed Forces and their support units securely connected. The Signal Corps is the Army's IT provider and remains integral to the Army's success.

**Pro Patria Vigilans!**



# New commander leads Cyber Center of Excellence

*By Kimberly Lewis*

Less than six months after its establishment, the U.S. Army Cyber Center of Excellence added another first to its growing record when MG Stephen G. Fogarty took command on 8 Sept. 2014.

MG LaWarren V. Patterson relinquished command of the Cyber CoE and Fort Gordon to MG Fogarty in the center's first-ever changeof command ceremony, held on Barton Field.

MG Patterson took command of the Signal Center of Excellence and Fort Gordon in July 2012.

Army leaders announced that the Cyber CoE would be established at Fort Gordon in December 2013.

The Signal CoE officially became the U.S. Army Cyber Center of Excellence in March.

"Fort Gordon, you have delivered in spades," said MG Patterson, who's heading to become the deputy commanding general for operations at Installation Management Command, Joint Base San Antonio, Texas.

"Our accomplishments together over the past two years have been nothing short of incredible. Since the unveiling of the Cyber Center of Excellence sign on 28 March, we have done in months what would normally take years."

"[MG Patterson] excelled and his working cyber into the center of excellence is really remarkable," said LTG Robert B. Brown, commanding general, U.S. Army Combined Arms Center and Fort Leavenworth, Kansas.

LTG Brown who presided over the ceremony said, "He often had to balance tough challenges and figure out the key aspects in an area with no history, uncharted territory and no past examples to rely on. "

" When I accepted command two years ago I had no idea how many significant events would happen during my tenure," Patterson said. "Now as I look back I'm amazed at how much has been accomplished as we worked together to make the Cyber Center of Excellence a reality. Fort Gordon,

(Photo by Bill Bengtson)

**During the change of command ceremony 8 September 2014, LTG Robert Brown, *(right)* commander U.S. Army Combined Arms Center and Fort Leavenworth, Kan., passes the colors to MG Stephen Fogarty, incoming commander U.S. Army Cyber Center of Excellence and Fort Gordon. With them are SGM Travis Cherry, *(left)* U.S. Army Cyber Center of Excellence command sergeant major and outgoing commander MG LaWarren V. Patterson.**

you have given me your utmost and I am proud of what we accomplished together."

MG Fogarty comes to Fort Gordon from Fort Belvoir, Va., where he was commanding general of the U.S. Army Intelligence and Security Command, but he's no stranger to the installation. MG Fogarty commanded NSA-Georgia and the 116th Military Intelligence Group at Fort Gordon from 2005 until 2007 and is returning after seven years to be the commanding general of the installation. He told attendees he's humbled and excited to be taking command, but realizes he has big shoes to fill.

"The biggest challenge right now is ensuring the Cyber Center of Excellence actually reaches full operational capability on the timeline that I have," said MG Fogarty.

"What we're going to have to do is come together in a way we really haven't in the past. Now I have to build on the momentum that [MG Patterson] created."

"This is all about (the Soldiers and family members)," he said. "They are the engine that truly powers everything that we are trying to accomplish. It's not just the Soldiers; it's actually [also] the very highly-skilled civilian workforce that we have, and they're completely supported by their families, and that's why our relationship with the local community is so important."

"The United States does not have a monopoly on cyber," MG Fogerty added. "We really have to take a bunch of different efforts that were scattered throughout the Army and ... finally bring them together. The coordination, the integration of a bunch of these efforts is really coming together right now."

(Photo by Bill Bengtson)

**MG Stephen Fogarty, incoming commander U.S. Army Cyber Center of Excellence and Fort Gordon, offers his first address after assuming command during change of command activities on Barton Field at Fort Gordon 8 September 2014.**

As a military intelligence officer MG Fogarty also addressed, speculation in the community that his assignment to command the Cyber Center of Excellence signals a diminishing prominence for the Signal Corps.

"I am aware that many of you are concerned about an intel officer taking this position," he said, drawing laughter from attendees. "Don't be! You will not find a stronger advocate for a strong Signal Corps than I. A robust, resilient and secure network is the critical enabler for effective mission command, fires, logistics, intel, medical, aviation, information operations and other important capabilities; and the network doesn't build, operate, maintain or defend itself. In fact, the network is not only an enabler but it is also a weapons platform. As we move forward, we must have a strong Signal Corps."

The assignment represents a homecoming for MG Fogarty, himself a native of Savannah, Ga. His mother was born in Augusta, and his wife Sharon is a native of Atlanta.

"This is a dream for a Georgia boy," MG Fogarty said "Both Sharon and I are very excited to return home."

***Kimberly Lewis,*** *command information officer, came to Fort Gordon in March 2014. She previously served at Fort Leavenworth, Kansas; Fort Campbell, Ken. and Fort Polk, La., as a Department of the Army civilian. She also served six years active duty as a military broadcaster.*

*In his own words*

# New Cyber commander outlines his vision

Greetings to our Signal and Cyber force!

Much has happened at the Cyber Center of Excellence since the last edition of the Army Communicator. This is a time of rapid change as we aggressively pursue the vision set forth by the Secretary of the Army and the Chief of Staff of the Army. As you are aware, the Cyber CoE achieved provisional status this past spring. This summer, we appointed our first Signal commandant and Cyber commandant, and opened the doors on the Cyber School Headquarters. Finally, this fall, the CoE will attain IOC status as we work towards our goal of FOC in October of 2015.

Two commandants were appointed on August 4th. COL Tom Pugh, the first Signal Commandant and 37th Chief of Signal, will have oversight on the training, leader development, and personnel within the Signal Regiment, and COL Jen Buckner, the first Cyber Commandant, will do the same for the Cyber and EW fields. In addition, both will provide valuable input to the Cyber CoE toward the development of doctrine, organization, materiel, facilities, and policy, as we fulfill our mission as the proponent for Cyberspace Operations, Signal Operations, and Electronic Warfare.

As I transition into command of the Cyber CoE, I am motivated by the challenges and excited about opportunities that lie ahead.

The United States and our allies are under persistent cyber attack by a range of capable state and non-state actors to include criminal gangs and terrorists. Given the importance of our global missions, DOD's dependence on secure and reliable networks has never been higher. Army networks are the vital enabler for mission command, intelligence, logistics, medical and administrative activities.

Our networks are subject to increasingly sophisticated attack and we must dramatically increase our defensive and offensive capabilities to ensure information dominance and protect our freedom of action. Cyber operations are inherently Joint, Interagency, Intergovernmental and Multi-national and in order for us to successfully operate in this environment we must collaborate effectively with a range of traditional and nontraditional partners to include industry and academia. As we educate and train our future Cyber and Signal Soldiers, we must ensure they leave the schoolhouse and arrive at their units fully capable of operating as part of a combined arms cyber team. They must be ready to join the fight immediately.

Producing highly capable Soldiers and Teams armed with the latest tactics, techniques and procedures is our core mission. Historically, the institutional Army has trailed the operational Army in the development and instruction of TTPs. Trained based on the last fight, our Soldiers reach the operational Army still in need of lengthy "on the job training."

The field of Cyberspace Operations is evolving at a far too rapid rate to continue this model. Our operational units do not have the time to retrain the soldiers we send to the force. Rather, the soldiers who graduate from the Cyber CoE must arrive at their units, relevant to the fight from the first day.

**MG Stephen G. Fogarty**

Here at the Cyber CoE, we will collaborate effectively with ARCYBER, our joint and interagency partners, industry and academia to identify and develop solutions to the challenges of Cyberspace Operations, Signal Operations, and Electronic Warfare at net speed. Our transition plan provides us with the opportunity to make great strides towards these ambitious goals. So keep an agile mindset throughout this important transition, engaging with us as we continue to evolve. I am personally asking each of you to provide us feedback on areas where you believe we are missing the mark and need to adjust.

I'm proud to be your commander. I look forward to getting to know you and working with you to accomplish this vital mission on behalf of our Army and our Nation!

**Uniting the Force/Defending the Nation!**

*Moving on*

# Future bright for the Signal Regiment

Signaleers,

I am excited to serve as senior advisor to the commanding general, leading the Cyber Center of Excellence to increasingly higher levels of technical competence and institutional effectiveness. I have been an NCO for 24 years. In every leadership position I've held—from team chief to command sergeant major—I've seen the impact that good NCOs can have upon a unit, as they push it to excel through standards-based, performance-oriented, battle-focused training.

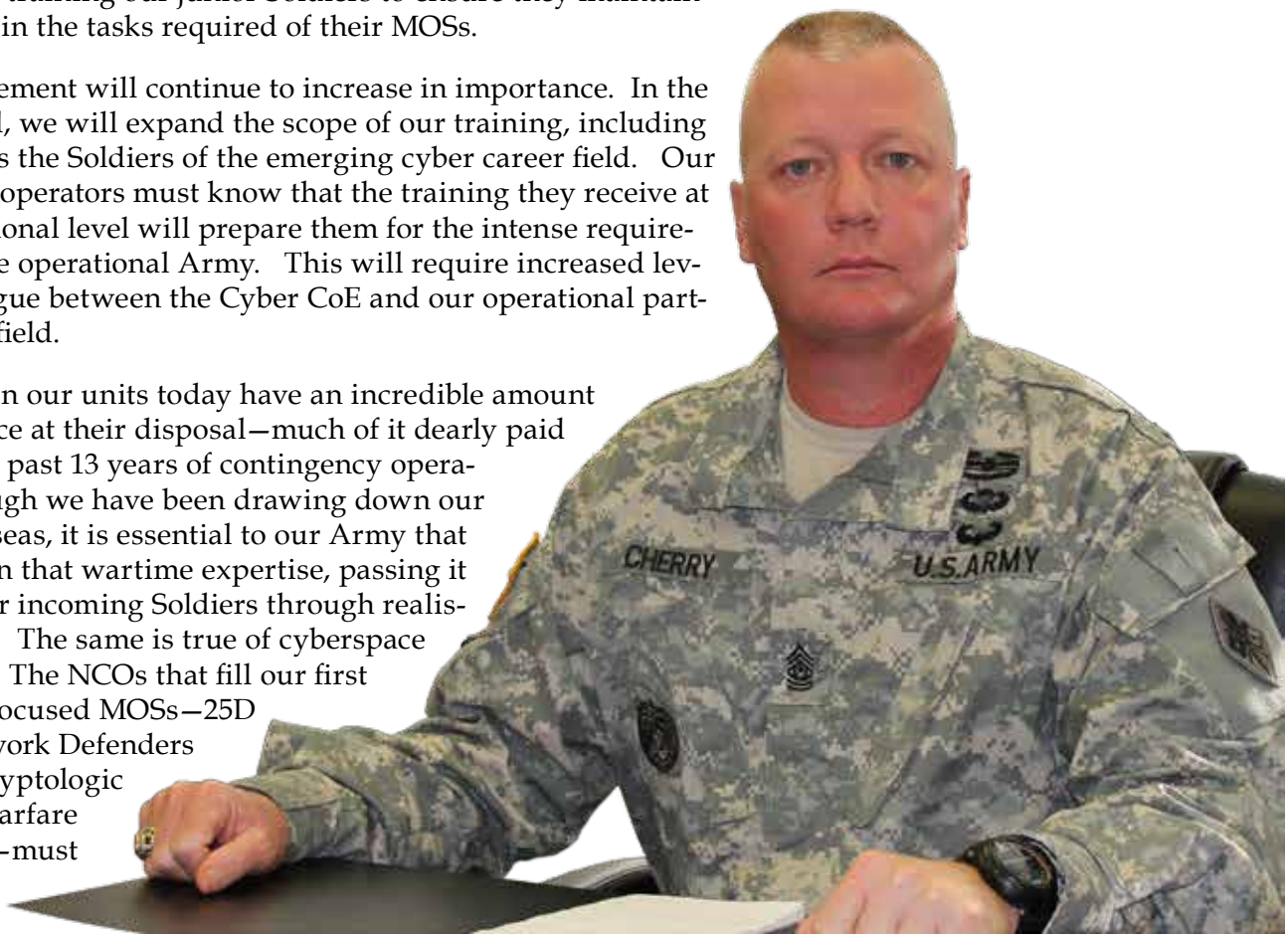
Training will become an even greater passion for me at the Cyber CoE. Here in the institutional Army, we are responsible for the initial training of all Signal enlisted Soldiers, as well as the professional educational required of our NCOs. But it is up to our operational NCOs to build upon the foundation we lay, mentoring our junior leaders and training our junior Soldiers to ensure they maintain proficiency in the tasks required of their MOSs.

This requirement will continue to increase in importance. In the years ahead, we will expand the scope of our training, including in our ranks the Soldiers of the emerging cyber career field. Our cyberspace operators must know that the training they receive at the institutional level will prepare them for the intense requirements of the operational Army. This will require increased levels of dialogue between the Cyber CoE and our operational partners in the field.

The NCOs in our units today have an incredible amount of experience at their disposal—much of it dearly paid for over the past 13 years of contingency operations. Though we have been drawing down our forces overseas, it is essential to our Army that we maintain that wartime expertise, passing it down to our incoming Soldiers through realistic training. The same is true of cyberspace operations. The NCOs that fill our first two cyber-focused MOSs—25D Cyber Network Defenders and 35Q Cryptologic Network Warfare Specialists—must use the skills and expertise they are developing to train the future cyber Soldiers that will fill their formations.

I am proud of the part I play in legacy and tradition the NCO corps has upheld as the backbone of the Army. Let us now redouble our efforts to train our Soldiers for the future. It is up to our NCO leaders to continue to identify the training required to achieve proficiency in our Soldiers' MOS-specific tasks.

**Pro Patria Vigilans!**



# Colorless core improves security, depth of network interoperability

*By Amy Walker*

The colorless core might sound like a "sci-fi" video game, but it's actually a highly secure network routing enclave.

Along with an advanced satellite network modem, the colorless core is part of a network upgrade that is improving the security, interoperability and efficiency of Warfighter Information Network-Tactical, the Army's tactical communication network backbone.

The WIN-T Increment 1b upgrade is the bridge for Increment 1 units to 'talk' more easily to units with Increment 2, said CPT Eric Michael Kilcullen, a company commander for the 86th Expeditionary Signal Battalion, which received the upgrade earlier this year.

"Additionally, the colorless core provides us that extra encryption so we can better support the Soldier," CPT Kilcullen said.

The Army is upgrading WIN-T Increment 1, which provides high-speed networking at-the-halt, with both the colorless core and the Network Centric Waveform modem, which optimizes bandwidth and satellite utilization. Both of these capabilities are already inherent in the more recently fielded, mobile WIN-T Increment 2 network. Although the pre-upgraded WIN-T Increment 1 can communicate with WIN-T Increment 2, having similar baseline equipment will facilitate more efficient communications between the two increments.

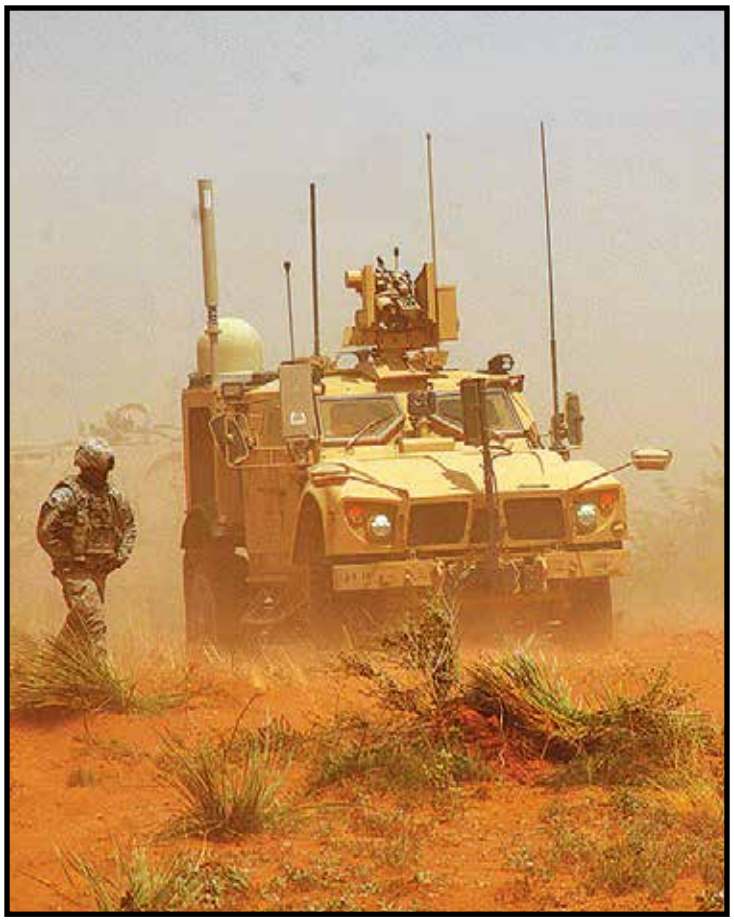
"The 1b upgrades are going to be huge for both the commanders and Soldiers on the ground," said MAJ Rickie Meers, 86th ESB operations officer. "They are going to be able to communicate earlier in the setup process and everything is going to work a lot smoother."

At the heart of the WIN-T Increment 1b upgrades is the addition of the colorless core routing enclave, which changes the network's encryption architecture and the way that encrypted information is transported over satellites and line-of-sight links. It enables Soldiers to send information across the battlefield more securely and efficiently than ever before, while optimizing bandwidth use.

The reason it is called

(Photo by Amy Walker)

**Soldiers from the 86th Expeditionary Signal Battalion prepare this Warfighter Information Network-Tactical Increment 1b Joint Network Node for a training exercise at Fort Bliss, Texas in February 2014.**



(Photo by Nancy Jones-Bonbrest)

**This Warfighter Information Network-Tactical Increment 2-equipped vehicle was utilized during the Network Integration Evaluation 14.2, at Fort Bliss, Texas in May 2014, which provided an increased coalition presence.**

"colorless" is that the Army often places color codes on certain security enclaves, with unclassified typically being designated as green and secret as red. In the colorless core no one can tell whether the encrypted information is secret or unclassified; the "color" cannot be identified.

"Look at it as a transport network," said CPT Stephan Wilson, C Company commander for the 86th ESB. "For example, a WIN-T Single Shelter Switch has NIPR, SIPR and coalition purple, and the colorless core can push all of that over one transport. It's going to allow us to push out a lot of different networks and traffic over one core so we can use our transport more effectively."

Additionally, the colorless core enables the Army to more easily add other enclaves to the network, such as 4G LTE/Wi-Fi and the Mission Network Enclave, a new network stack that can be rapidly reconfigured to provide tactical access for one of four different networks: the coalition network, SIPR, NIPR, or commercial internet and phone service.

Along with the colorless core, the WIN-T Increment 1b upgrade also takes advantage of the NCW through the addition of an NCW modem for satellite transmission. NCW is a dynamic and on-the-move capable waveform that optimizes bandwidth and satellite utilization. Since it is used by Increment 1b and 2, NCW facilitates direct transmission and increased interoperability between the two versions of the network.

"The new modem self-heals; it power balances itself and tries to achieve the maximum throughput without operator input," said WO3 Keith L Hudson, 86th ESB network technician, responsible for implementing the components and assemblages in the tactical network. "We won't have to worry about the modem and its performance unless something drastically goes wrong."

The WIN-T Increment 1b upgrades are being fielded through a regional training site approach, a more cost efficient and timely alternative to traditional unit site upgrades. Initial efforts for the upgrades began in January 2012 and are over 50 percent complete to date. Not only will the upgrades improve capability and interoperability with WIN-T Increment 2, but they also add operational flexibility to the network.

"With all the different units, missions and types of equipment out there, whether WIN-T Increment 1 or 2, the upgrade makes it a lot easier for the commanders on the ground to be able to plan and execute their missions," MAJ Meers said. "Interoperability is not going to be a second thought; it's just going to work without having to figure out all the different network configurations."

**(Continued on page 10)**

(Continued from page 9)

Fielded to approximately 90 percent of the Army, WIN-T Increment 1 has been supporting a full range of military operations since 2004 and provides Soldiers at the battalion level and above with at-the-halt, high-speed, high-capacity voice, data and video communications. WIN-T Increment 2 adds on-the-move access to the tactical network down to the company level and extends the network over vast distances and difficult terrain, further connecting Soldiers in geographically separated locations.

Going forward, units such as ESBs whose requirements can be satisfied with at-the-halt networking capability will retain the upgraded WIN-T Increment 1 equipment, while those units where mobility is critical to mission success will receive WIN-T Increment 2. Because the Army is delivering these upgraded capabilities to units on a staggered schedule, there may at times be "hybrid" network architectures on the battlefield that include WIN-T Increments 1a (the pre-upgraded equipment), 1b and 2.

WIN-T Increment 1b units will be able to talk directly to Increment 2 units with minimum lag and optimum results. Until all Increment 1a units receive the 1b upgrade, they can still effectively communicate. An Increment 1a unit can talk directly to an Increment 1b unit. It can also talk to an Increment 2 unit via division headquarters Tactical Hub Nodes or one of five worldwide stationary Regional Hub Nodes. This transport method adds lag time and is slightly less efficient in bandwidth use, but it is reliable.

Along with the colorless core and the NCW modem, WIN-T Increment 1b and Increment 2 also share the same baseline set of Network Operations tools, although Increment 2 NetOps tools have additional capabilities. NetOps tools facilitate the planning,

(Photo by Amy Walker)

**Soldiers from the Army's 86th Expeditionary Signal Battalion train on Warfighter Information Network Terminals upgraded with WIN-T Increment 1b advancements, at Fort Bliss, Texas in February 2014.**

(Photo by Lawrence Holgate)

**Soldiers train on a Satellite Transportable Terminal at a Regional Training Site in Fort Drum, N.Y. Upgrades to Warfighter Information Network-Tactical WIN-T Increment 1 are being fielded through a regional training site approach, a more cost efficient and timely alternative to traditional unit site upgrades.**

initialization, monitoring, management and response of the network. Having similar tools increases the capability and interoperability of current and future network increments.

Capability gaps between Increments 1 and 2 will be further minimized when the Army completes its current NetOps convergence efforts, aimed at simplifying and reducing the number of network management tools its communication officers use to manage the network. Once these efforts are complete, the different increments will be able to share network management. This will allow the service to mix and match task organizations, to potentially insert an Increment1 battalion into an Increment 2 unit or provide more Increment 2 equipped infantry to an Increment 1 equipped brigade as needed, said John Shotwell, technical management division chief for Product Manager WIN-T Increment 1.

"As far as working with your support units, the Increment 1b upgrade is critical," Shotwell said. "ESBs, sustainment brigades, maneuver enhancement brigades and similar units will have Increment 1b as a baseline, so if they are going to support Increment 2 at the tip of the spear, they will be on the same common communications backbone."

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

## Acronym QuickScan

**ESB** - Expeditionary Signal Battalion
**NCW** - Network Centric Waveform
**NetOps** - Network Operations
**NIPR** - Non-secure Internet Protocol Router
**SIPR** - Secure Internet Protocol Router
**WIN-T** - Warfighter Information Network-Tactical

# The National Security Agency's host mitigation package initiative

*By MAJ Paul Meaux and Kevin Corbitt*

The ability to maneuver computer network defensive capabilities in today's environment has been limited by the adversary's command of modern technology and proficiency in exploiting vulnerabilities.

The constant introduction of new applications and platforms – coupled with the exponential increase in computing power – creates an enormous challenge for system administrators to adequately defend against malicious activity taking place on the network.

Detection of any new threat is often discovered only after data has been exfiltrated or other artifacts of an attack have been identified.

The normal response to any successful attack is to develop and deploy tools that will oppose that specific threat.

However, that approach is reactionary in nature and does nothing to counter sophisticated adversaries that can easily overcome this type of signature-based response strategy by making simple modifications to their code.

A proactive way forward that focuses on prevention rather than reaction is needed. In response, the National Security Agency has initiated a host mitigations package designed to aid organizations and system administrators in hardening their host systems.

## Host Mitigation Package Overview

Most organizations tend to focus mainly on securing the larger network. Devices such as firewalls, routers, and intrusion detection and prevention systems get most of the attention from network administrators.

Although securing the network is vital, hardening host systems is just as essential and deserves the same level of consideration. Planners and developers within the Department of Defense are working to address emerging host threats by implementing capabilities like the SANS Top 20 Security controls.

However, this DoD effort is being deployed in stages and NSA leadeers have determined that a single, comprehensive program regarding host hardening must be developed.

NSA proponents initiated the HMP in order to corral the many disparate security controls into one, easy to deploy package. The HMP supports the defense-in-depth strategy in which multiple layers of security controls are placed throughout a host. Any single layer of defense will most certainly contain gaps that could be exploited by an enemy.

A series of different security defenses residing in a single host should be used to cover the gaps in other layers. The intent of HMP is to not only prevent security breaches, but also to buy an organization time to detect and respond to an attack. As such, an adversary that is not stopped cold will have to work harder and longer, thus reducing and mitigating the consequences of a breach.

The HMP uses an effective combination of operational tools designed to provide a layered defense against the most common and most effective techniques utilized by hostile actors.

These tools mutually support each other with overlapping security boundaries. This package was designed to implement existing commercial software to provide low resource cost with high gains in overall system security. The HMP uses the following tools and configurations:

1. Application Whitelisting
2. Microsoft's Enhanced Mitigations Experience Toolkit
3. Pass-the-Hash Protection
4. Anti-Virus Cloud Lookup
5. Host-Based Security System

Each of the tools mentioned above has a subject matter expert at the NSA who provides independent testing and documentation on proper deployment and configuration methods that are shared with the customer.

The HMP team lead works closely with industry partners

to provide relevant security features in order to continually improve HMP products.

## Application Whitelisting

All applications can introduce unknown and unacceptable security risks to any host or network. AWL is a proactive security technique where only a limited set of approved programs are allowed to run. By default, all other programs – including most malware – are blocked from running. AWL prevents the use of unauthorized applications, thereby limiting the attack surface to only security risks that the organization has chosen to accept. In contrast, the standard policy enforced by most operating systems allows all users to download and run any program they choose.

AWL is only one layer in the defense-in-depth strategy and is not a replacement for traditional security software such as antivirus and host firewalls.

For an AWL solution to be effective, all executable code must be blocked by default, so that only approved programs can run. Users must not be allowed to modify the files that are permitted to run. AWL enables administrators, not the users, to decide which programs are allowed to execute.

### *AWL Advantages*

1. Blocks most current malware.
2. Prevents use of unauthorized applications.
3. Does not require daily definition updates.
4. Requires administrator installation and approval of new applications.

## Microsoft's Enhanced Mitigations Experience Toolkit

EMET is a host-based application that hooks into processes and watches for common memory exploitation techniques like buffer overflow attacks. These common attacks use vulnerabilities present in un-patched versions of Adobe Reader, Flash Player, and other Internet applications. When EMET detects an exploit attempt, it promptly kills the targeted process, logs the attempt, and notifies the user that it has shut down the application. EMET can provide a layer of retroactive protection by safeguarding applications in cases where new zero-day exploit events have been discovered and patches have not yet reached the host. EMET's true value is in stopping common attacks like those seen in drive-by downloads and black-hole infected sites.

EMET is a free application and can be deployed using typical enterprise deployment methods. Once deployed, maintenance is very low, although some time must be taken to monitor and resolve possible compatibility issues that could arise. The NSA has developed guidance on effective deployment and maintenance strategies.

### EMET Advantages

1. Stops attacks at the exploit stage before any payload can be delivered.
2. Stops common drive-by download attacks.
3. Requires the adversary to change their exploits to bypass it; increasing their costs and lowering success rates.
4. Is simple to deploy and easy to maintain.
5. Adds another layer to a defense-in-depth strategy at a very low cost.

## Pass-the-Hash Protection

PtH is a hacking technique that allows an attacker to authenticate to a remote system by using the underlying Windows NT or LAN Manager Hash of a user's password, rather than having to know the actual password.

The operating system generates a hash of the account password for use in single sign-on operations so that the user is not prompted to enter their credentials each time access to a resource is requested. This hash is passed legitimately by the operating system for authentication. PtH uses these legitimate hashes to illegitimately authenticate to a system. PtH has become a general name for an entire range of related credential theft and reuse attacks that affect most authentication systems contained in modern operating systems.

PtH is commonly used by attackers to gain greater privileges in order to carry out increasingly devastating attacks and to exfiltrate data. Some of the mitigation techniques for PtH include: restricting and protecting high privileged domain accounts; restricting and protecting local accounts with administrative

**(Continued on page 14)**

(Continued from page 13)

privileges; and restricting inbound traffic using a firewall.

There are 4 main goals for PtH Protection:

1. Keep usable forms of credentials off of computers when they are not actively in use. In other words, no current logon session with those credentials.
2. Always keep usable forms of sensitive credentials off of less sensitive computers.
3. Limit the time that a usable credential is valid for access.
4. Limit the scope that a usable credential is valid for access (e.g., domain administrators are denied login to user workstations).

## Anti-Virus Cloud Lookup

The majority of technologies currently in use to detect malicious activity on DoD networks rely on signatures of "known-bad" activity or files. This approach is very easily defeated by small modifications to malicious files or through innovative new techniques. Recent advances in anti-virus technologies – including those provided to the DoD by vendors such as McAfee and Symantec – leverage a "cloud lookup" capability in which files can be referenced against a global reputation database to discover new potentially malicious activity and report to system administrators for follow-on remediation. This capability is alternatively referred to as File Reputation Lookup and Cloud Heuristics.

Additionally, McAfee and Symantec have proprietary names for their capabilities: GTI and Insight, respectively.

AV applications get the most up-to-date intelligence about suspicious files or activities by reaching back into the cloud. This reach back provides near real-time protection of the endpoint against new and emerging threats and improves the security posture of the Department of Defense Information Network. This capability provides protection to the hosts above and beyond what is offered by existing signature files. AV Cloud lookup can serve as protection from new malicious files until they are incorporated into enterprise deployed signature files. For example, GTI detects specific instances of malware as opposed to classes of malware, which significantly reduces the chances of generating false-positive detections.

## AV Cloud Lookup Advantages

1. Protection against newly discovered malware can be initiated within seconds, versus the hours or days required for updating host detection via signature files.
2. Provides mechanisms for better control over every file entering the network, helping to control network hygiene, which is one of the most pressing network defense challenges.
3. Better positions DoD personnel to respond to fast moving attacks that could hobble operations across the Non-Secure Internet Protocol Routed Network.
4. Has a lower false positive rate than existing McAfee.DAT files.
5. Provides 10% to 30% better detection than signature DAT files alone.

## Host-Based Security System

HBSS is the official name given to the DoD commercial-off-the-shelf suite of software applications used to monitor, detect, and counter attacks against DoD computer networks and systems. The Enterprise-wide Information Assurance and computer Network Defense Solutions Steering Group sponsored the acquisition of the HBSS System for use within the DoD Enterprise Network. HBSS is deployed on both the NIPR Network. The goal is to have HBSS configured on every server, desktop, and laptop within DoD.

HBSS is centered on McAfee's ePolicy Orchestrator management engine and consists of several point products. A point product is an individual software application that is controlled by the ePO. McAfee point products include the following: Host Intrusion Prevention System, Policy Auditor, Assets Baseline Module, Rogue System Detection, Device Control Module, and the Asset Publishing Service.

## HBSS Advantages

1. Has capability to block unknown intrusion signatures and restrict unauthorized services and applications.
2. Ensures compliance with statutory and regulatory requirements.
3. Addresses system baseline configurations and reacts to changes in the Information Operations Condition.
4. Provides real-time detection of new hosts attaching to the

network.
5. Ensures application patching compliance.

## NSA Support to HMP

The HMP is modular and can be tailored to fit customer needs. For example, one of the major combatant commands approached the NSA and was interested in implementing HMP during a high-profile annual exercise. This combatant command already had HBSS on a segment of their network and had previously implemented AWL. The NSA provided EMET and PtH configuration assistance and was able to complete the entire HMP. This combatant command received a mature computer network defense hardening and NSA demonstrated that HMP can be rapidly deployed with tangible gains in network and host-based security.

There are no costs to obtain the tools that are part of the HMP. They are either system configurations or freely available commercial or Government-off-the-Shelf software and are available for immediate download. System administrators should expect about two weeks to "tune" the software for optimal performance across their network. The HMP suite of tools works with the standard baseline of Windows XP, Windows 7, or Windows 8 operating systems.

The NSA has published configuration guides in order to help organizations interested in the HMP initiative. These configuration guides outline the steps and correct system settings necessary to properly employ the HMP. These guides will be enhanced and updated on a periodic basis in response to advances in technology or adversary tactics. In addition to the configuration guides, the NSA can provide training support during both the install and tuning period.

The Information Assurance Directorate at the NSA is also developing mitigations packages for the network, identity protection, and enterprise services. Once these packages are complete, they can be deployed in conjunction with the HMP to provide an added layer of protection across the entire enterprise. The complete series of mitigations packages are designed to help system administrators successfully defend their networks against a wide range of malicious attacks.

## Summary

Malicious attacks against DoD networks are increasing every year. In order to help system administrators combat these attacks, the NSA has developed a mitigations package that focuses entirely on the host. This Host Mitigations Package assembles a series of tools that share overlapping security boundaries in order to provide defense-in-depth protection against an attack. These tools and configurations are easy to use and deploy with little to no cost. For more information or to request support, visit the NSA's website at www.nsa.gov website for the appropriate points of contact.

***MAJ Paul Meaux*** *is an FA24 and is the Army client advocate for the Information Assurance Directorate of the National Security Agency.*

***Kevin Corbitt*** *is a mitigations analyst for the Information Assurance Directorate of the National Security Agency.*

## ACRONYM QuickScan

**AV –** Anti-Virus
**AWL –** Application Whitelisting
**DoD –** Department of Defense
**DODIN** - Department of Defense Information Network (formerly identified as GIG--Global Information Grid)
**EMET –** Enhanced Mitigations Experience Toolkit
**ePO –** ePolicy Orchestrator
**HBSS –** Host-Based Security System
**HMP –** Host Mitigations Package
**NIPRnet** - Non-Secure Internet Protocol Routed Network
**NSA –** National Security Agency
**PtH –** Pass-the-Hash
**SIPRnet –** Secure Internet Protocol Routed Network

# Signal officers leveraging LEAN 6σ sigma

*By CPT Asheesh Nikore*

As Signal officers, our master of core competencies within the technical field, be it automation, strategic or tactical communications, or on the cyber front, are essential to do our jobs proficiently.

Staying in tune to this technical edge that is ever changing is a constant learning effort and takes dedication to first grasp a skillset and then fine tune it with application. Signal officers constantly acquire new skillsets in our tool bag and repertoire.

Vendor certifications such as CISCO, Juniper, or Microsoft or other certification bodies such as ISACA, Comp TIA, and ISC2 offer many IT Certifications coupled with experience help substantiate a skillset.

However, just applying the skillset doesn't always translate to success. Some efforts are multifaceted projects with variables and complexities that have interwoven dependencies which require a team approach and management of specialized skills to reach a final successful milestone.

Additionally, we are often evaluated and graded on how our IT initiatives perform in an environment of limited resources and fiscal constraints. Therefore, two additional ingredients that prove valuable in one's military progression and have a proven track record are Project Management and Lean Six Sigma.

As Signal officers progress in their military career, they rely more heavily on their IT project management skills. Junior officers exercise their abilities of general project management on a smaller scale with planning and leading of physical training, weapons qualification events and command exercises.

First, how does one define a project?

A project can simply be defined as a temporary endeavor designed to produce a unique product or end result with a defined beginning and end. The ultimate success is shaped and dependent on what is called the triple constraint. The triple constraint is comprised of the factors of schedule, budget and scope.

As any one of the three factors change the other two are impacted.

For example, if one's lifecycle replacement FY budget for the network architecture is slashed; its scope has a positive correlation in that the number of backbone routers that can be refreshed decreases. The schedule could be impacted adversely as well. The nature of the public sector may seem less stringent then the private sector, but nonetheless the same constraints are encountered.

Project management discipline provides an understanding of the required sequential activities and processes in an efficient phase approach along with certain valuable concepts throughout the process. The five main phases are initiating, planning, executing, monitoring and controlling, and closing.

Projects are not managed in a vacuum as many resources are dependent on different entities and different stakeholders have a vested interest in the project's success.

How your organization is structured (Functional vs. Projectized such as a Project Management Office) will influence how you negotiate for resources, do business, and gain leadership support. Typically military units are functional without a PMO and have department leads (i.e. your S2 or G2, G3, G4, G6, et. al.) Two key mathematical models critical to ensure one's project is managed successfully and in control are the Critical Path Method and Performance Evaluation and Review Technique.

The critical path method allows one to determine which activities in your project schedule have zero float and therefore those activities are the most critical to your project schedule. PERT is a mathematical formula that allows one to guesstimate activities durations and resource requirements to have more accuracy to assist in planning. If one is behind schedule, fast tracking or crashing, are two ways

accelerating progress but with added risk and resources.

One great example of an IT project is certification and accreditation of networks using the Risk Management framework of the DoD Information Assurance Certification and Accreditation Process. In this process the information assurance manager implements several controls based on sampling and quality checks. As IT planners and PMs in the Signal arena, delivering projects of quality and value on time translate to our ultimate mission; supporting the warfighter.

A key subset of project management is quality. There are certain quality metrics and thresholds that may be required and come from one's industry, organization, or maybe a regulatory compliance. What Lean Six Sigma combines is quality (minimize variation) with speed to support business transformation in its operations. It achieves this in a systematic tollgate approach using statistical methods, root cause analysis, and tools to minimize waste and non-value added activities and therefore enhance process improvement via efficiency. The LSS concept originates from quality assurance practices of eliminating defects (non-value added) to 3.4 defects per a million opportunities and one of the bedrocks of quality is continuous process improvement.

There are five phases to include define, analyze, monitor, improve and control. LSS-qualified candidates are belt based depending on one's level of training. LSS can be applied by a Signal officer because there are many opportunities in which LSS can assist. Any process that is numbers driven can probably achieve effeciencies through the LSS methodology. Help desk queues, IT procurement process, release and change management, data backup processes, cloud virtualization strategies, transmission signal flow, and asset management are just a few examples in which LSS can prove value in the Signal arena.

I had the unique opportunity as a green belt qualified LSS practitioner and project manager of the a communications facility data center to apply the LSS principles to our project's lifecycle process and improve its maturity. By using the LSS principles, I was able to determine where the process wasn't in control, apply a solution and test via a pilot phase, and provide mitigation measures to increase efficiency in the process and government savings by cost avoidance and increased man hour utilization.

Coupling both the Project Management and LSS disciplines in approaching IT projects as Signal officers will yield dividends and support new ways to determine best practices. In our present fiscally constrained environment where one has to do more with less and increase the return on the investment, leveraging ways to increase our results with limited resources is critical for successful results.

As Signal officers, leveraging these skills in our projects' day-to-day operations and cementing them in standard operating procedures and processes will serve as force multipliers creating a more efficient and transformative environment. Project management and LSS will continue to play major roles in both our Signal careers and the entire military organization.

***CPT Asheesh Nikore*** *serves as an S6 at the 92nd Chemical Battalion. He deployed and completed a tour as the MCF Data Center project manager and project portfolio officer in charge for the G3/7 projects. He has completed the following IT certifications: CISSP, Network +, Security +, Project +, CEH, ITIL Foundation, and CompTia Green Strata certification.*

## ACRONYM QuickScan

**CPI** - Continuous Process Improvement
**CPM** - Critical Path Method
**DPMO** - Defects Per a Million Opportunities
**DIACAP** - DoD Information Assurance Certification and Accreditation Process
**LSS** - Lean Six Sigma
**PERT** - Performance Evaluation and Review Technique
**PMO** - Project Management Office

# Gunslingers complete mission

*By CPT Thomas A. Allen*

The 534th Signal Company, located at Fort Carson, Colo., has a rich history embedded in the 43D Sustainment Brigade motto "Making it Happen."

Routinely, the company is called upon to conduct signal operations and support across Fort Carson, to both organic units and adjacent units.

Recently, the 43D Sustainment Brigade was notified that it will most likely become NORTHCOM's active duty Sustainment Brigade to support natural disaster missions.

With that mission, comes huge responsibility including providing sustainment logistical operations and communication operations. The brigade was contacted by NORTHCOM to conduct an exercise with the 534th Signal Company, "Gunslingers," 43D Sustainment Brigade.

This exercise was much more than just a regular signal certification exercise (usually called a digital CERTEX) that is conducted on a quarterly basis. This mission will eventually have an impact on hundreds of thousands of people, including the military, civilians, agencies, and corporations around the country.

The ability to provide internet to commanders on the battlefield in a combat environment is essential to the success of today's Army. What about when that "mission" is here on our homeland in the United States? That is exactly what the 534th Signal Company was able to accomplish from 9 DEC – 13 DEC 2013.

The 534th Signal Company was the first unit, let alone the first Signal company, to push commercial, NIPR, and SIPR internet through military equipment.

Additionally, the company was able to establish NIPR and SIPR internet giving the military and DA civilians the secure connections needed to accomplish their missions.

The Joint Network Node, known as the JNN, and the Command Post Node, known as the CPN, is equipment is organic to the military and most Signal companies in the Army today. It is the same equipment that is usedacross the forces worlwide. This equipment was used during the CERTEX to test the commercial NIPR, SIPR push.

When a natural disaster hits America, the military provides the resources and support to communities that need critical assistance. These resources can be provided to the communities even faster with the response of an active duty sustainment brigade. The 534th Signal Company provides the communication resources that enable various government agencies and civic/commercial organizations to communicate.

Additionally, this connectivity impacts police and fire departments to ensure baseline services throughout the disaster area. With all of the human service needs evolving in a homeland mission it is critical to have police and fire departments connected with the community to be able to deliver emergent services.

With sustainment and communications established early and effectively, the community leadership can have access to hundreds of assets with hours. Cellular phone use is limited during a natural disaster and the cell phone network/civilian network infrastructure is far too congested to be effective.

Internet, provided by the 534th Signal Company and 43D Sustainment Brigade can benefit both the civin organizations but also the individual citizens of the community. Friends and families will be able to communicate faster and find missing persons.

The Soldiers of the 534th Signal Company are the ones that provide the technical knowledge, long hours, and dedication to mission to make the CERTEX a success. It was truly a team effort.

With the help of the brigade network operations section and S6, the mission was a great success.

The Soldiers of the company are always ready when called upon and will make anything happen.

198th Expeditionary Signal Battalion

# Technical control facility closure

*CPT Jeff Stevens*

The 198th Expeditionary Signal Battalion provided unparalleled communications support to the warfighter during their 2013 – 2014 deployment to Afghanistan. The ESB provided tactical satellite communications, network operations expertise, and cable and wire services.

This National Guard battalion, comprised of three units in Delaware and a fourth in South Carolina, was presented with a unique challenge; learning how to successfully close a technical control facility. The battalion met this daunting task with detailed preparation and coordination, effectively closing four TCFs in the process.

A TCF provides network services to large user bases in tactical and strategic environments. Email, file storage, phone routing, Host Based Security System, Active Directory and Domain Name System are key services delivered to users while deployed tactically. A TCF can be fixed or modular and mini to medium sized. A mini TCF can service up to 4,000 customers, while a medium can service up to 20,000. During this deployment, the 198th ESB retrograded four modular TCFs; three minis and one medium.

During the initial

**(Continued on page 18)**

(Photo by CPT Jeff Stevens)

**Example of mini technical control facility divided in half in order to ship off-site. The missing section is a mirror image of the rightmost displayed section. A TCF supports NIPR, SIPR, and CX-I services. Also pictured is a portion of the air conditioning and cooling system located below the TCF.**

(Continued from page 19)

preparation of a closure, it's imperative that the Battle Space Owner is intricately aware of all facets of the plan and what impact there will be on warfighter communications. The challenge is to ensure user's services are not interrupted during their migration to either local or regional hub sites.

In order to accomplish this, a temporary set of computer servers and file servers must be created from scratch with theater provided equipment. The data stack is configured to each site's specific needs and deployed at the tactical out site where the TCF in question was identified for retrograde. Redundant fiber and Category 5/5e/6 network cable must be run from every location at the forward operating base to the new data stacks; all while ensuring the TCF network remains intact.

Once redundant services and connections are established on site, the Signal community within the Regional Command comprising the TCF determines if the installed custom data stack will provide enduring services, or if a portion or all of those services will be fully migrated to a major hub site. There is a level of risk with not terminating network services locally. If the FOB is nearing complete closure; then it's more practical to migrate services to a distant hub and prepare for a complete closure at that location.

The TCF goes dark and all network connections removed when all site services are properly transferred. Once dark, a 198th ESB retrograde team augmented by SPAWAR, SERCO and CENTURUM contractors arrive to dismantle the TCF. Though planning allows for several weeks for these actions, an efficient team, under the right conditions can dismantle a TCF in four to five days and have the site totally clear. Proper planning with the network migration enables the retrograde team to work quickly at inventory, tear down and shipping processes.

## Spin Boldak TCF Closure

The Spin Boldak TCF closure presented our team with a unique set of challenges. First, the FOB had an unlabeled cable backbone, built by multiple units over several years. After years of operation and more than a dozen units stationed on this FOB, the network was a complicated mess.

How do you replace the main communications node in a FOB, while providing seamless service, if you do not know where any of the wires leaving that node are going? The FOB experienced constant fiber breaks due to unmarked cables being dug up and cut which resulted in loss of services. Further, the improper labeling increased the threat of Cross Domain Violations. The situation was unpredictable.

A cable and wire team was dispatched two months in advance of the TCF closure in order to properly test, label, and map the network diagram for the FOB. They worked 12-16 hour days between four team members to map and record every single wire going into and out of the TCF. It was painstaking, but necessary.

The cable and wire mission consisted of a second critical objective; properly connecting all FOB locations in a logical manner and clearly labeled.

Redundant fiber connections were redesigned and new physical network nodes were established throughout the FOB in order to facilitate a meshed star topology. There was over 40,000 feet of networking cable run to accomplish this task. The network now made sense.

Concurrent with the cable and wire mission, a 198th ESB Network Engineering (NetEng) team was creating a data stack for deployment to the FOB. The data stack consisted of all the networking equipment, file storage, and computing power required to provide file, voice, email, and print services on site locally. It was determined that HBSS, Active Directory, and DNS services would be migrated to Kandahar Airfield. The migration of those services to Kandahar would be

complete before the data stack was deployed.

After two months of cable and wire migration, and one month of assembling and configuring the custom data stack; the site was prepared to transfer services locally. The new data stack was sent out with both a NetEng and Enterprise Operations Team. The NetEng team was responsible for connecting the stack to the network and ensuring all connections to customers were complete. The EntOps team setup the services and ensured that the local communications team was properly trained on its operation. The cable and wire team was on stand-by to repair any connections that may have been overlooked during their two months of preparation.

Within one full week of concurrent operation with the data stacks providing primary services and the TCF providing back-up services, the mission was declared a success and the TCF went dark. Cables were cut between the TCF and the FOB. The data stack was now the primary communication node for the FOB. A 198th ESB retrograde team arrived to dismantle the TCF within four days. Spin Boldak's TCF closure was a complete success without interruption in services to the warfighter.

## TCF Closure Lessons Learned

There are a few lessons learned from the 198th ESB's four TCF closures.

First, a cable and wire team should be dispatched as early as possible with a representative from the NetEng team building the data stack. Collaboration between the cable team and the engineers were crucial in order to develop a logical migration plan.

Depending on the state of the fiber network at the FOB, the cable and wire team must be on site anywhere from two weeks to two months. There was a large difference in network maturity and complication between FOBs. No two are alike.

A second lesson learned was ensuring users were properly informed. Scheduling Authorized Service Interruptions were key in informing FOB and regional Signal Corp leadership. It is very important to develop face-to-face relationships with major FOB customers and Battle Space Owners. In our case, the 198th ESB site OIC/NCOIC would personally engage key combatant commanders to inform them on the network status. Information is an essential part of customer service.

The third and final lesson learned was the knowledge that developing a well rounded team of Soldiers with skills in network, movement and heavy equipment operations resulted in total success. Proper planning and team building result in TCF that are seamless during retrograde operations.

***CPT Jeff Stevens*** *served as the assistant S3 for the 198th Expeditionary Signal Battalion (Delaware Army National Guard) under Task Force Signal, 160th Signal Brigade in Kandahar, AFG.*

## Acronym QuickScan

**CDVs** - Cross Domain Violations
**DNS** - Domain Name System
**EntOps** - Enterprise Operations Team
**ESB** - Expeditionary Signal Battalion
**FOB** - Forward Operating Base
**HBSS** - Host Based Security System
**KAF** - Kandahar Air Field
**NetEng** - Network Engineering
**TCF** - Technical Control Facilities
**TPE** - Theater Provided Equipment

# Technical control facility in a box offers transitional benefits

*By SPC Derek W. Kinhofer*

The Technical Control Facility in a Box is a transitional, portable, and modular system that is assembled in transit case configuration for physical assembly.

The TiB was conceptualized in 2007 from a need to have a temporary modular communications package for the drawdown in Iraq and Afghanistan. TiBs were built to maintain communications while the strategic Technical Control Facilities were decommissioned. The TiB is comprised of 37 transit cases and can support up to 500 users concurrently. The TiB is used as a more permanent solution when transitioning from a Joint Network Node. It provides an improved communications capacity until a more permanent infrastructure is designed and implemented. Unlike the TCF or mini TCF; power, heating, ventilation, and air conditioning are not integrated.

The TiB provides multiple services utilizing Black Core transport architecture in accordance with CENTCOM enterprise fielding guidance. Services and application hosting is virtualized and complies with Information Assurance/ Computer Network Defense controls.

Locally hosted servers are exchange, local authentication for expedited login, file share, and call manager. Services provided are NIPRNET, SIPRNET, and Combined Regional Information Exchange. Transport for the services is provided using either AN/USC-60 or Deployable Ku-Band Earth Terminal system.

Using either antenna system the TiB sets itself apart from the Warfighter Information Network-Tactical dynamic as it is designed for a stationary forward operating base. While WIN-T systems can be rapidly deployed, such as the SIPR/NIPR Access Point which is able to be moved by a Light-Medium Tactical Vehicle, the TiB has to be planned for transitions from a standing headquarters FOB or become the main network transitioning from the WIN-T systems.

## Submit an article to the *Army Communicator*

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

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

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

***How to submit an article***

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

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

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

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

However, the TiB can still be a member of the WIN-T family as it has the ability to serve as a headquarters for stable tactical sites or a hub for outlying tactical terminals.

While WIN-T equipment gives the Tactical Commander more flexibility and maneuverability on the battle field; the TiB is able to provide greater services to the end user at the theater level. Another benefit of utilizing the TiB compared to WIN-T equipment is when units RIP in or out the end user does not see any changes to their actual devices. When WIN-T equipment is replaced different equipment, Internet Protocols, and phone numbers will change at minimum; with the TiB, the IPs and phone numbers are in place until the TiB no longer serves its function.

The TiB is used in theater to provide reliable communications for CENTCOM Forward Elements. With the growing scope of the Jordan mission as well as missions in South West Asia it makes sense to utilize the TiB because it is suited to grow with, and meet the demanding needs of all its users.

The TiB has two recommended minimum manning requirements. For missions less than ninety days, a minimum of five personnel is required. If the mission requirement is more than ninety days, the minimum personnel required is eight. Through experience with this system lower manning requirements put a strain on regular maintenance, due to also having helpdesk support requirements.

The team consists of a team chief, information systems operator/analyst, satellite operator/maintainer, and a nodal network systems operator. The team chief position is held by either a 255A or 255N warrant officer, or a 25B40. Server and help desk support is provided by two 25B Soldiers for missions less than 90 days and manned by three for missions greater than 90 days. Installing the antenna requires either a 25S or 25Q. Two is recommended for missions greater than ninety days. The 25N or network operator is required to configure and remediate issues within the network. Two 25Ns are recommended for longer missions.

Cross training personnel is essential because all team members need an understanding of all positions. Doing this provides the capability to give Soldiers a rest and recuperation day, eliminating single points of failure across the team. As the population on the network grows, it is essential to have more helpdesk personnel to remediate the larger number of user issues. Establishing a ticketing system is essential to keeping track of Local Area Network issues and providing reliable services to the end user.

As a forward operating base grows so does the need for reliable communications, this is where the TiB is able to shine as the transitional setup before becoming a permanent solution. As an FOB shrinks, the TiB again is a solution to provide reliable communications while the main TCF is being decommissioned. A TiB has the capability of providing a multitude of services as well as assisting on the WIN-T infrastructure.

***SPC Derek W. Kinhofer*** *is a 25S satellite communications operator and maintainer. He has obtained the CompTIA A+ and CompTIA Security+ certifications.*

## ACRONYM QuickScan

**CENTRIX** - Combined Regional Information Exchange
**DKET** - Deployable Ku-Band Earth Terminal
**FOB** - Forward Operating Base
**IA/CND** - Information Assurance/Computer Network Defense
**JNN** - Joint Nodal Network
**LMTV** - Light-Medium Tactical Vehicle
**TCF** - Technical Control Facilities
**TiB** - Technical Control Facility in a Box
**WIN-T** - Warfighter Information Network-Tactical

# High capacity line-of-sight solution

*By CW2 Angel Gonzales*

This article outlines methods I have used to successfully deploy the Combat-Service-Support Automated Information Systems Interface as an alternate means to achieve High Capacity Line of Sight connectivity for WIN-T Increment 1a/b nodes.

The purpose of this paper is not to compare all available commercial line of sight systems, but a few comparisons will be made.

## Background

By default, the "CAISI" – also referred to as the Fortress ES520 Deployable Mesh Point – is nothing more than a sustainment information system used to securely extend NIPR services provided by the CSS-VSAT via wireless bridge. I set out to deploy the CAISI with the intent of supporting the WIN-T network architecture during our National Training Center rotation 14-08. The purpose was to supplement or replace the High Capacity Line of Sight shelter, which the Brigade had very few of.

In order to feasibly support the entire Brigade Combat Team, to include enablers via LOS, I would need HCLOS shelters placed at each BN Command Post and possibly each RETRANS site.

This would also require additional equipment and manning from each BN S6 and logistical support for those teams. This COA; however, was not feasible due to personnel and equipment allocations.

So here enters the CAISI. Its IP based radio is capable of providing excellent throughput and extending to distances beyond any challenge the NTC landscape presented. To be specific the CAISI is capable of link speeds of up to 50Mbps with an average latency of <1ms – 4ms and can establish links at distances of up to 35 miles between nodes when using the directional grid-antenna.

The CAISI uses the Fortress Security Suite of encryption protocols exclusively for link establishment on Antenna# 2 (the antenna we would be using). The CAISI is very similar to another COTS IP radio currently in use across the Army today, the Harris RF-7800W-OU440. A few similarities are displayed in the table below at the bottom of this page.

| Radio | Fortress ES520 | Harris RF-7800-OU440 |
|---|---|---|
| Performance | Sustained FIPS Crypto Throughput<br>- 50Mbps | >90Mbps PTP<br>>45Mbps PtMP |
| Range | Up to 35 Miles or 56km | >90km clear LOS PTP<br>>45km clear LOS PtMP |
| Security | FIPS<br>- FIPS 140-2 Level 2<br>Encryption<br>- AES-CTR-128/192/256<br>- AES-GCM-128/256<br>- AES-CCM-128<br>- IPsec<br>- NSA Suite B Upgradeable | FIPS 140-2 Level 2<br>256-bit AES |
| Management | HTTPS, Console, SSH, SNMP | HTTP, HTTPS |
| Environment | Operating Temperature<br>- -10°C to +55°C (14°F to +131°F)<br>Storage Temperature<br>- -37°C to +72°C (-35°F to +161°F) | Operational<br>- -40°C to +60°C |
| Certification | Safety & Emissions<br>- CE, FCC, ETSI, CB Test, IC, RoHS<br>Environmental – RoHS-6<br>DFS – FCC, ETSI<br>NIST – FIPS 140-2 level 2<br>JITC – UCAPL Certified<br>Wi-Fi Alliance – Wi-Fi a/b/g<br>Weather Resistance Protection Rating<br>- IP56, NEMA 4<br>- Watertight Enclosure<br>- Lightning Arrestors | FIPS 140-2 Level 2 Certified |

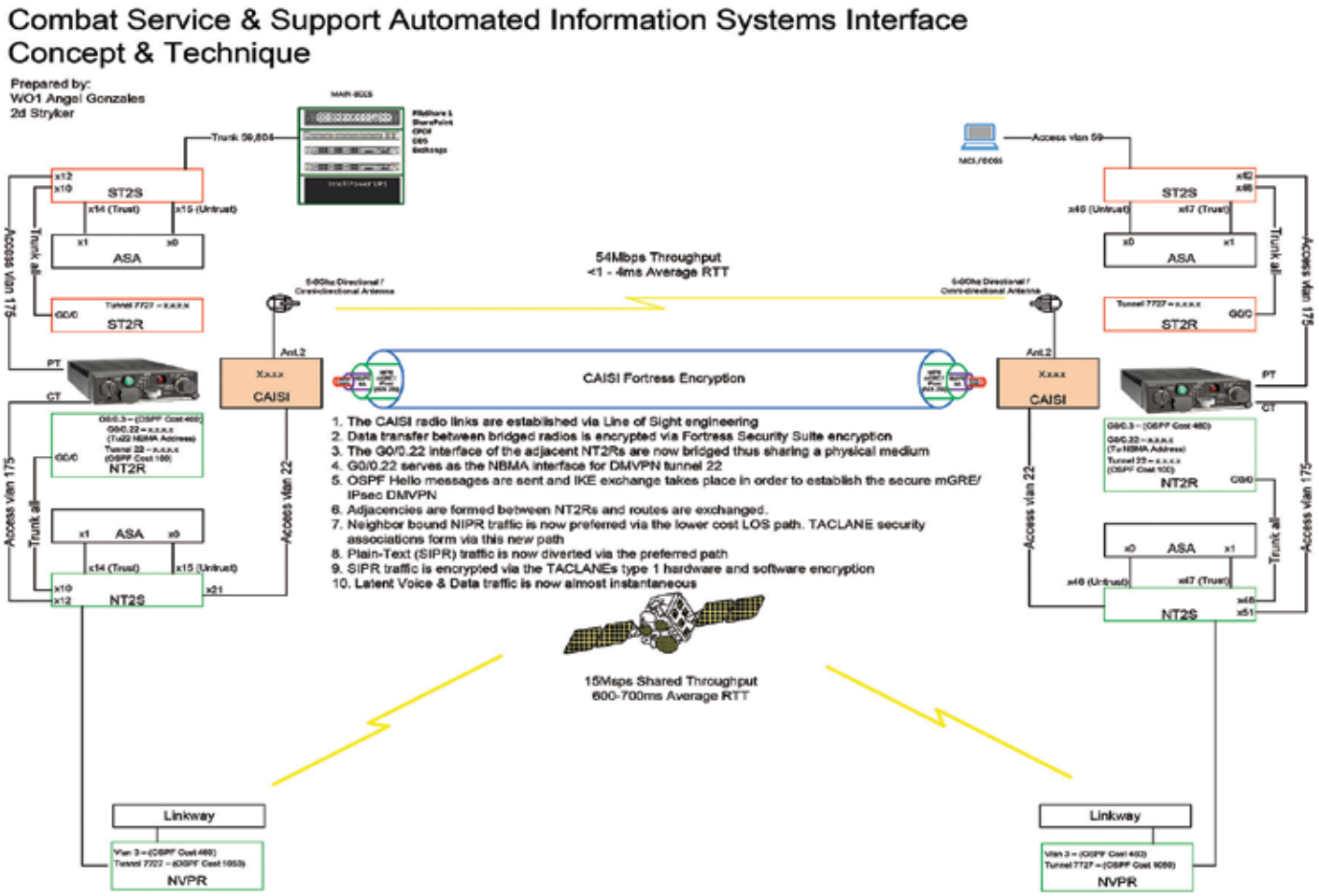
The CAISI also boasts easy implementation. For the planned network architecture the CAISI would require a minimal amount of operator training for setup and link establishment.

When inquiring about the amount of CAISIs the brigade owned, the unit SASMO informed me that we had exactly 71 of them distributed across the brigade, with two at each company, battery or troop. SAMSO's plan to support the sustainment mission included the S1, S4, and aid station at each battalion. This however, did not include the Infantry line units.

## The Physical Network

We were headed into a decisive action fight which meant battalion TOC locations would adjust as the fight progressed. The network would also need to be adjustable and support engineering ad-hoc links regardless of a unit's position. The CAISI would be engineered to share a common frequency spanning the entire LOS mesh which made frequency allocation simple.

Each battalion S6 officer was tasked to resource two radios minimum from within their respective units. HHC's/




HHT's/HHB's radios were hands off due to sustainment mission requirements. Each radio acquired was capable of providing a PTP or PtMP link(s) and would be attached to an OE-254 pole set, QEAM antenna or 15m mast (if available). This would enable each BN to effectively create links and RETRANS if necessary. The resulting physical layout of the network was very flexible, but in most cases was a combination of a physical-star and a physical-bus topology.

## The Logical Network

I chose to implement a DMVPN for the LOS architecture. This would support any ad-hoc network additions and provide ease of administration. The radio's Ethernet connection would be provided via the NT2S, which could also power the radio if the power-injector or supply was missing or faulty.

I created a common VLAN which was instated on all NT2Ss. The switch interface connecting to the CAISI was configured to provide access to this new VLAN. A new sub-interface was created on GigabitEthernet 0/0 of each node's NT2R in order to process the encapsulated traffic. Each sub-interface was allocated an IP address from a spare subnet sourced from the unit IP scheme. With all radio links established, this design placed all NT2Rs in the same broadcast domain. I also created the DMVPN tunnel interface on the NT2R and assigned it an IP from a separate and specific subnet. The NT2Rs new sub-interface subsequently became the NBMA address for the DMVPN tunnel.

I chose to place the tunnel on the NT2R – a Cisco 3825 Integrated Services Router - as opposed to the NT2S to ensure that all traffic from the Data/Voice/Netmgmt/IA subnets would continue to route through the respective firewall contexts once the LOS DMVPN had established. I also wanted to add a layer of data protection and integrity via IPsec, in addition to the strong link encryption already provided natively within the CAISI radio. IPsec protection and DMVPN interfaces were two critical features to the design that the Cisco 3560G (NT2S) just didn't support.

**(Continued on page 26)**

(Continued from page 25)

In order to provide maximum redundancy and compatibility between nodes, the OSPF priority on each of the BN's LOS tunnel interface was left at the default of 1. I did this to allow any two or more adjacent BN nodes to establish full OSPF adjacencies and also exchange routing information. If the priority was set to 0, as is on the NVPR, it would result in neighboring nodes forming bi-directional adjacencies. Although an adjacency is formed, no routing information is exchanged due to the absent DR/BDR. There is an advantage to allowing the BN nodes to conduct election of a DR/BDR amongst themselves without the JNN present. If a node's primary transport (AN/TSC-167Fv1 or 2) goes down for maintenance or malfunction, NIPR traffic from that node is then completely rerouted via the LOS link.

This provides a fast, secure and low latency NIPR path for direct communication to adjacent nodes. The OSPF cost on the LOS tunnel was also set to 100 so it becomes the preferred path. This is important for NIPR core architectures as TACLANE SAs will establish via this new path. Once the SAs have established, nodes begin to form adjacencies via the SIPR DMVPN tunnel over LOS. Voice and Video communications become almost instantaneous to include critical mission command systems, common operational picture and enterprise services alike. An example of the physical/logical connections and deployment technique can be seen in the graphic onpage 25.

***CWO2 Angel Gonzales*** *has served as the network management technician for the 2d Stryker Brigade, 2d Infantry Division, Joint Base Lewis-McChord since May 2013. Prior to his appointment as a warrant officer (255N), he served as the brigade network operations NCOIC for 2d Brigade, 82d Airborne Division, Fort Bragg, N.C. from June 2009 to September 2012. CW2 Gonzales' technical education includes certifications: CISSP, CCNP, CCNA, CCENT, CompTIA Security+, CompTIA Network+, CompTIA A+,MCSE, MCSA and MCP. CW2 Gonzales graduated the Network Management Technician Warrant Officer Basic Course 255N on 2 April 2013.*

## Acronym QuickScan

**AES –** Advanced Encryption Standard
**BDE –** Brigade
**BDR –** Backup Designated Router
**BN –** Battalion
**CAISI –** Combat Service Support Automated Information Systems Interface
**CB –** Certification bodies
**CBC-MAC –** Cipher Block Chaining Message Authentication Code
**CE –** European Conformity
**CCM –** Counter with CBC-MAC
**COA –** Course of Action
**COTS –** Commercial Off The Shelf
**CTR –** Counter Mode
**CSS-VSAT –** Combat Service Support Very Small Aperture Terminal
**DFS –** Dynamic Frequency Selection
**DR-** Designated Router
**DMVPN –** Dynamic Multi-Point Virtual Private Network
**ETSI –** European Telecommunications Standards Institute
**FCC –** Federal Communications Commission
**FIPS –** Federal Information Processing Standards
**GCM –** Galios/Counter Mode
**HCLOS –** High Capacity Line of Sight
**HHB –** Headquarters and Headquarters Battery
**HHC –** Headquarters & Headquarters Company
**HHT –** Headquarters & Headquarters Troop
**HTTPS –** Hyper Text Transfer Protocol Secure
**IC –** Industry Canada
**IP –** Internet Protocol
**IPsec –** Internet Protocol Security
**IP56 –** Ingress Protection (Dust & Water)
**JITC –** Joint Interoperability Test Command
**JNN –** Joint Network Node
**KM –** Kilometer
**LOS –** Line of Sight
**MBPS –** Mega Bits Per Second
**M –** Meters
**NBMA –** Non-broadcast Multi-Access
**NEMA 4 –** National Electrical Manufacturers Association (Watertight)
**NETMGMT –** Network Management
**NIPR –** Non-secure Internet Protocol Router
**NIST –** National Institute of Standards and Technology
**NSA –** National Security Agency
**NT2R –** NIPR Tier 2 Router
**NT2S –** NIPR Tier 2 Switch
**NVPR –** NIPR Virtual Private Network Router
**OSPF –** Open Shortest Path First
**PTP –** Point to Point
**PtMP –** Point to Multi-Point
**QEAM –** Quick Erecting Antenna Mast
**RoHS –** Restriction of Hazardous Substances
**RETRANS –** Retransmission
**SASMO –** Sustainment Automation Support Management Office
**SIPR –** Secure Internet Protocol Router
**SNMP-** Simple Network Management Protocol
**SSH –** Secure Shell
**STT –** Satellite Transportable Terminal
**TOC-** Tactical Operations Center
**UCAPL –** Unified Capabilities Approved Products List
**WIN-T –** Warfighter Information Network-Tactical

# Gateway Telecommunications Center, Modernized Enterprise Terminal dedicated

*By 1LT Genevieve Jarrett*

(Photo by SGT Ernesto Gonzalez)

***(From left to right)* LTC Billy Miranda, 302d Signal Battalion commander; LTC Kim Bivin, 21st Signal Brigade deputy commander; LTC Brad W. Endres, U.S. Army Corps of Engineers, Baltimore District deputy commander; CPT Benjamin Custer, 298th Signal Company commander; COL Clyde E. Richards, Jr., Defense Communications and Army Transmission Systems project manager; and COL Steven P. Middlecamp, U.S. Army Garrison Fort Detrick commander cut a section of a ribbon during the indoor portion of the Modernized Enterprise Terminal dedication at Fort Detrick, Md., 14 May, 2014.".**

The 21st Signal Brigade, 302nd Signal Battalion, 298th Signal Company hosted a ribbon cutting ceremony to dedicate the 298th Signal Company's Gateway Telecommunications Center and Modernized Enterprise Terminal on 14 May2014 at Fort Detrick, Md.

The command teams of the Baltimore District of the Corps of Engineers, Project Manager - Defense Communications and Army Transmission Systems, and the past commanders of the 298th Signal Company attended the ceremony in support of the current commander as they cut a section of the ribbon to symbolize the transformation from old to new technology.

The newly constructed GTC is a functionally reliable, consolidated state-of-the-art telecommunications facility used to support Presidential and Joint Chiefs of Staff command and control, communications, and intelligence requirements.

The building project to create a modern telecommunications center began in 2010. While in construction, the 298th Signal Company decommissioned its aging AN/FSC-78 Satellite Communications Terminal, which is being replaced with a much more capable AN/GSC-52B(v)2/G MET terminal. The Technical Control Facility is also being upgraded in a major way by converting to an "everything over Internet Protocol" concept.

The GTC combines the Technical Control Facility and the Satellite Communications Facility into a single 33,700 square foot building. The facility operates seven days-a-week, 24 hours-a-day and provides space for wideband critical communications equipment supporting worldwide military and commercial satellite communications. These systems provide a primary transmission path for high capacity and protected communications supporting the Warfighter at all levels of command and control. The completion of this construction project culminates over a decade of intense planning and execution.

# It's Time to Get Ready for Cyber War

*By LTC Frank Beyer*

***Editor's Note:*** *A similar version of this article was originally published in the German professional journal "Antenna" and is reprinted in the Army Communicator to invite creative thinking and comments from readers. The described activation and reorganization measures for the Cyber Center of Excellence have been and are being modified since this article was published in Germany in August 2014. The opinions and conclusions expressed are those of the author and are not official doctrine or policy of either the U.S. Department of Defense or the German Department of Defense.*

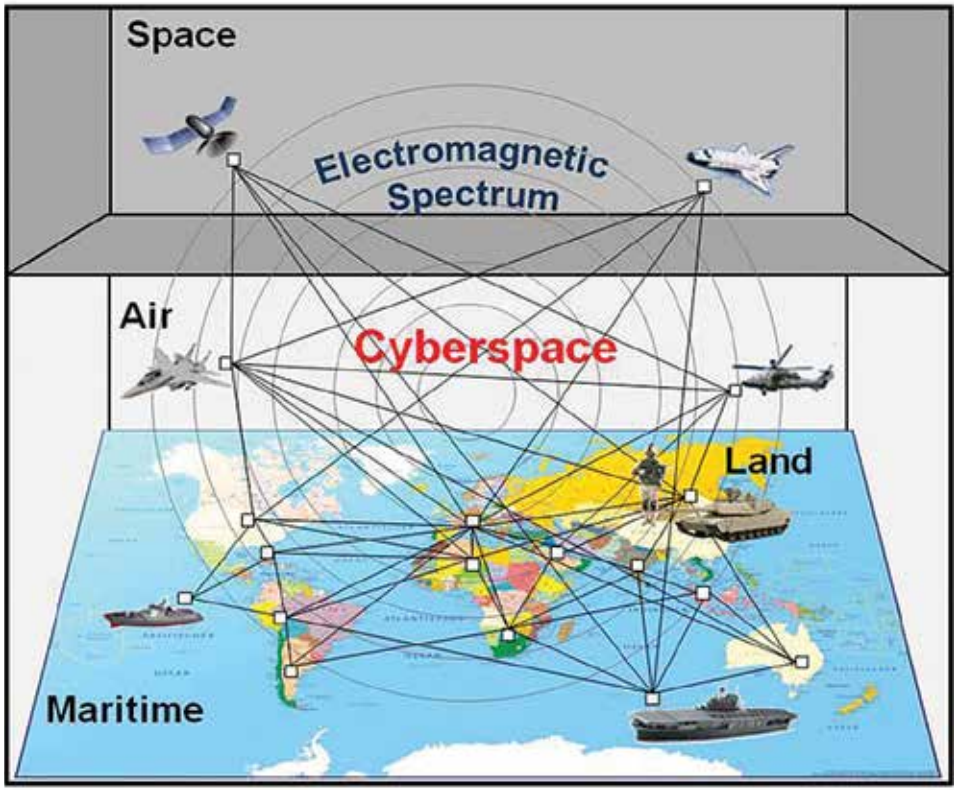



**Figure 1 Operational Domains**

The United States, the U.S. military and, in particular, the U.S. Army consider the Cyber Domain to be at least as important as the classic domains of land, air, sea, and space. Despite considerable cuts in the U.S. defense budget, accompanied by extensive force downsizing, efforts are under way to achieve a considerable, mutually coordinated capability gain in the Cyber Domain.

The German Federal Government, too, describes in its Cyber Security Strategy paper the utilization of the Cyber Domain and the integrity, authenticity and confidentiality of the information contained therein as one of the existentially important issues of the 21st century.

The present article, using a comparison of current approaches, capabilities, and developments of both countries in the Cyber Domain, attempts to identify possible fields of action at the military level from a German perspective.

## Military not prepared for threat of cyber attacks

"What we're seeing in cyber is going to continue and it's going to grow and it's going to get worse.

The platform we have today is not defensible. You can't see it, you can't defend it, and I would guarantee you that the adversary could penetrate it. And it'd take us months to find it.

One of the biggest challenges we face is a military culture in which separate branches can't share information. We have a signal community that builds, operates and defends our network at the secret level, and we have a national community and an intelligence community that exploits and provides the ability to attack at the top secret level. The things that top-secret operators know about the network they don't share with people at the secret level because they're not cleared. That

would be like telling them 'you're going to get hit, can't tell you about it.' That doesn't make sense. Step one is to bring them together as one team. I stress the importance of training all cyber and signal personnel to the same standards and building a secure network infrastructure at a central location."

With the above risk assessment, former Commander of the U.S. Cyber Command, General Keith B. Alexander, announced a reorientation in the Cyber domain (quoted from an address given on 31 January 2013 at the Pentagon). Striving to protect national interests, this reorientation aims to expand the existing capabilities considerably, in particular by complementing the previously defensively oriented Cyber measures with offensive measures, while concurrently harmonizing the necessary training.

To implement these guidelines, the U.S. Department of Defense took the following decisions, which due to the expected costs, required the approval of Congress.

- Relocation of the U.S. Army Cyber Command to Fort Gordon, Georgia,
- Establishment of a U.S. Army Cyber Center of Excellence by using assets of the U.S. Army Signal Center of Excellence at Fort Gordon.
- Establishment of a new Cyber Electromagnetic branch in the U.S. Army, while creating various specialty and assignment categories for all careers.

## U.S. Army Cyber Center of Excellence

On 28 March 2014, in the presence of dignitaries from politics, the military and industry and trade as well as a huge number of media representatives, the U.S. Army Signal Center of Excellence was renamed the Cyber CoE.

Activation and reorganization measures for the Cyber CoE are governed by the organizational procedures as provided by the D.O.T.M.L.P.F. In the following, I am using this principle to describe the current status of affairs in order to provide an overview of current and future intended capabilities.

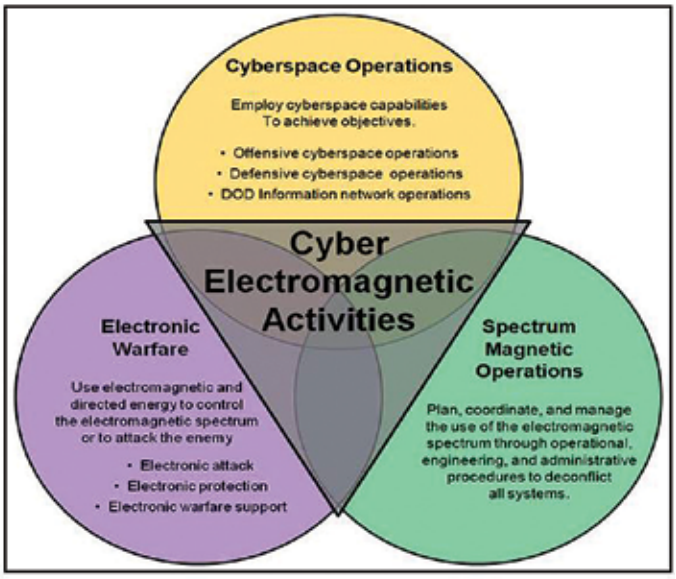



**Figure 2 CEMA**

## Doctrines and Concepts

So far, the cyber capabilities required from the point of view of the U.S. military have been laid down in two major documents open to view by Bundeswehr personnel.

Put into force at the Department of Defense level on 12 February 2014, the Cyber Electronic Activities document describes both the importance, objectives, measures and responsibilities, and legal basis of CEMA; furthermore, it presents their integration, synchronization and the doctrinal principles in the context of the C2 process, up to and including guidelines for the issuance of orders for the use of CEMA in operations abroad. (See Figure 1 on page 40 and Figure 2 above).

The "U.S. Army's Cyberspace Operations Concept Capability Plan 2016-2028" is the U.S. Army's policy document on the "Use of Cyber Operations as a contribution to successful Full Spectrum Operations". Figure 3 on page 42 shows the tasks and nature of cyber operations.

At the Department of Defense level, work is currently in progress on the "Army Cyber Space Operations" and "Joint Cyberspace Operations" documents. These documents are addressed to the military leaders and provide answers to the

**(Continued on page 30)**

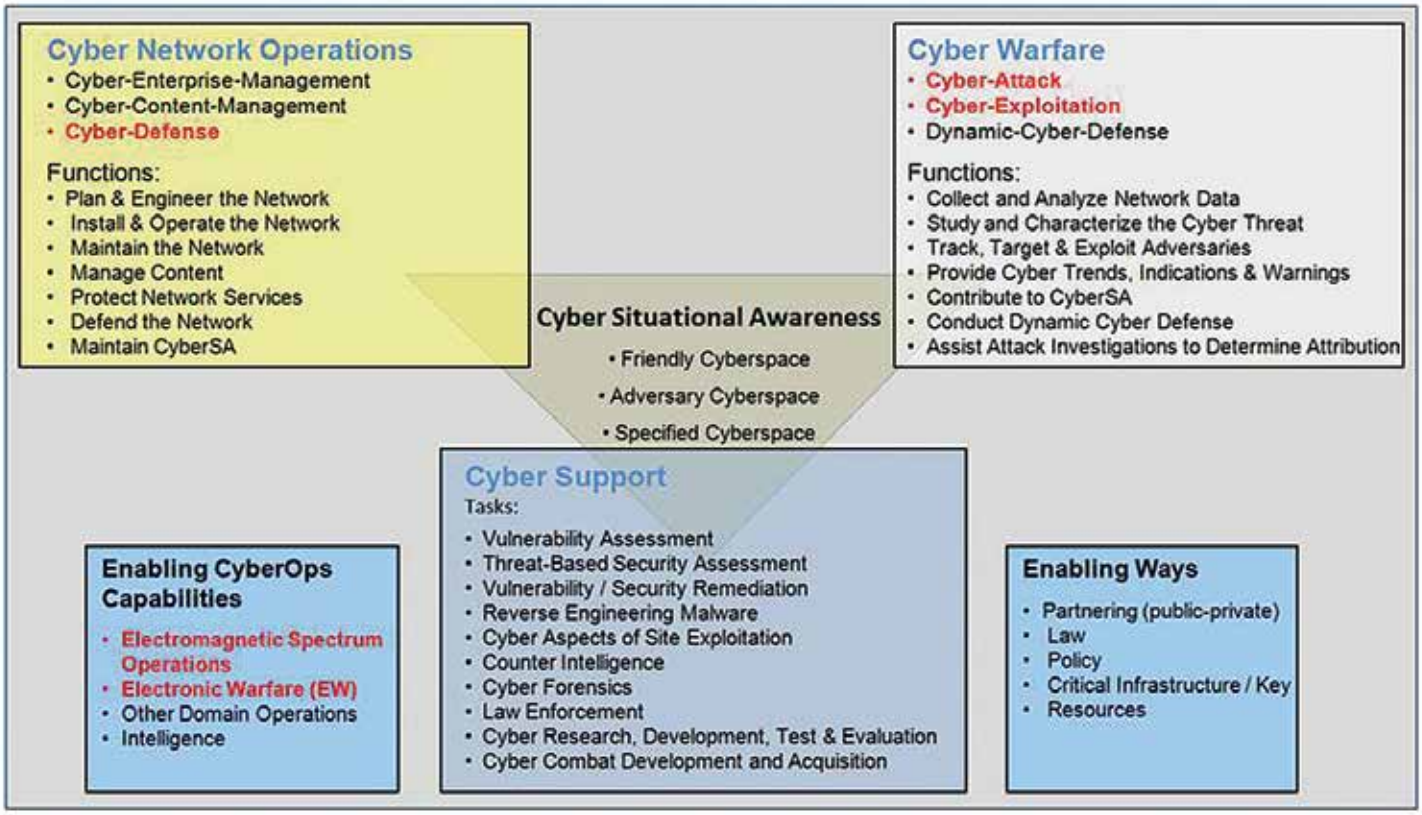



**Figure 3 Cyber Operations and Functions**

**(Continued from page 29)**

question: What do you want cyber to do for you?" Both documents are classified as US SECRET.

The documents "Capabilities-Based Assessment", the "Stationing Plan" and the CONPLAN prepared by the Cyber CoE are awaiting DoD approval and are crucial as a basis for financing and establishing Full Operational Capability.

## Organization

The restructuring towards Cyber CoE will occur in three phases. In the provisional phase (until 30 Sep 2014), the responsibilities in the Cyber Domain will be delineated towards other military agencies and institutions as well as government authorities, while conceptual work will be completed and the new C2 organization adopted. Instructions have been issued to reach Initial Operational Capability by 30 Sep 2015, aiming to implement new "Joint Cyber Offense" training programs. FOC (by 30 Jun 2016) focuses on finishing the work for new facilities and the completion of the reception and integration of ARCYBER from Fort Meade (See Figure 4 on page 31).

## Training

In addition to the training programs for communications and information systems support, further training courses for all career categories have already begun in the field of Cyber Defense. The development of Cyber Offense training programs is ongoing.

Starting in 2015, to be better able to meet the special Cyber challenges, the career category of branch officer will be established in addition to the warrant officers, the "classically" trained (CIS support, Cyber) line officers and enlisted. This new Army branch and career field will have available the same career prospects as a Operations

functional category officer to include command assignments.

The personnel trained along these lines will subsequently be placed under the management of the newly established Cyber Electromagnetic branch.

## Materiel, Leadership and Education, Personnel, Facilities

After relocation of ARCYBER and other intelligence units to Fort Gordon and personnel augmentation at the Cyber CoE, the number of military and civilian personnel of currently 22,000 will increase to a total of about 30,000. The costs, mainly for infrastructural work, are estimated at 160 million dollars.

## The U.S. Army is on its way

The U.S. Army already has extensive Cyber Defense capabilities to counter threats emanating from the Cyber Domain; these capabilities will soon be complemented by further goal-oriented measures, particularly in the fields of organization, procedures, training, and Cyber Offense.

By selecting Fort Gordon as the future home of ARCYBER and Cyber CoE, and with the 7th Signal Command's intelligence units and the National Security Agency Georgia, for the first time CIS, intelligence and EW assets required for impacting on the Cyber Domain will be under unified command, while military agencies, institutions and government agencies will be co-located.

**(Continued on page 32)**

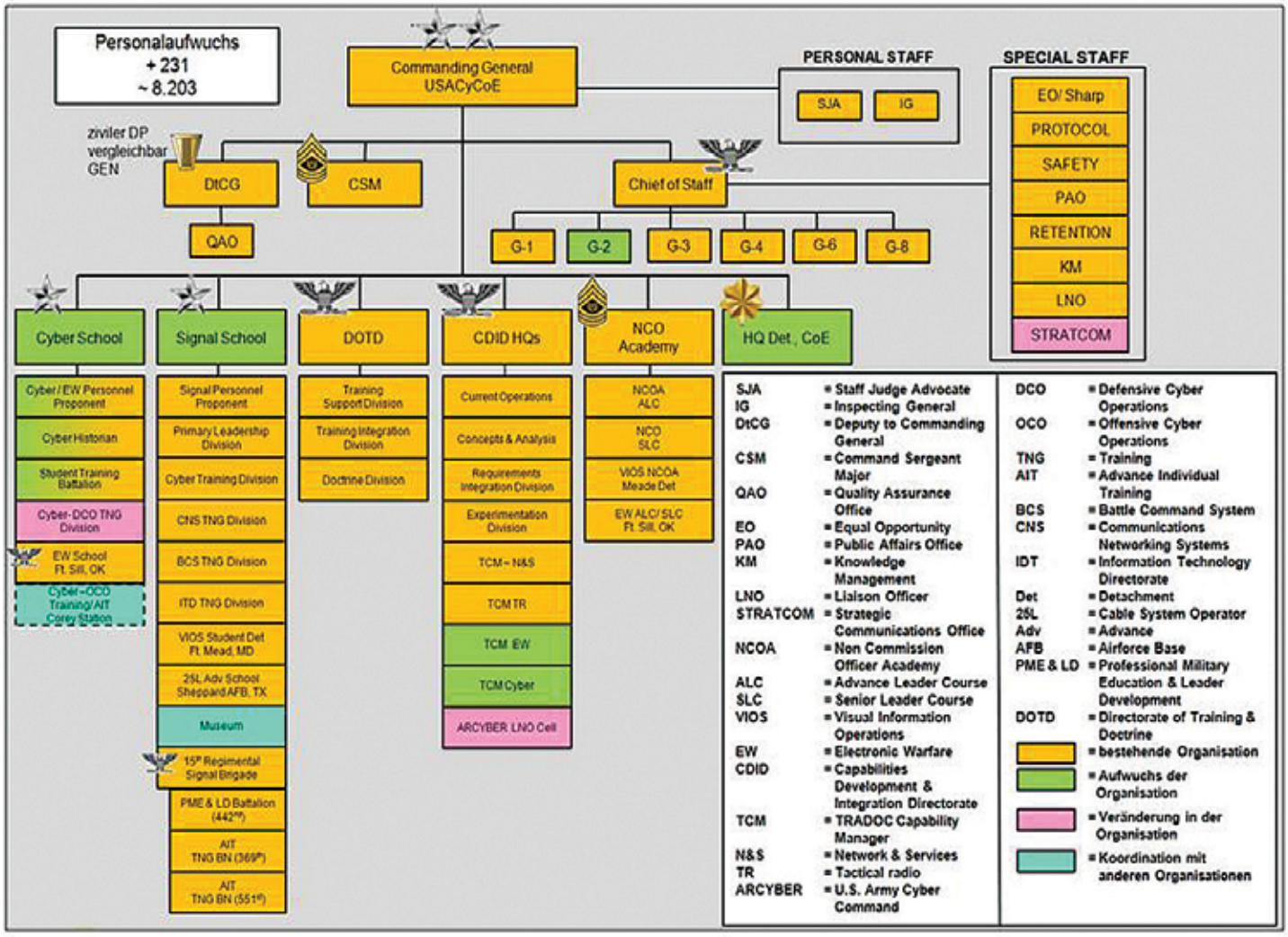



**Figure 4 Organizational diagram Cyber CoE**

(Continued from page 31)

This will create consistently improved conditions for operations planning and execution, training, further development, and for a coordinated interagency effort of several agencies active in the Cyber Domain.

## Cyber Security in Germany

The Cyber Security strategy paper drafted by the German Federal Government describes cyber security as a central, common challenge for the nation, industry and trade as well as civic society in the national and international contexts.

In contrast to the USA, the German Federal Government pursues an inter-ministerial, comprehensive approach, intensification of information exchange and prioritization of civilian efforts and measures. The Bundeswehr's measures are designed to protect its own capability for action in the context of underlying mandates and thus make cyber security an integral part of preventive national security.

The Federal Office for Information Security is responsible for the protection of the federal administration against Cyber threats and for developing guidelines on the protection of critical infrastructures in Germany. Once the BSI has assessed an IT crisis to be of an alarming or national scope, the IT Situation Centre, following buildup, will assume the role of IT Crisis Reaction Centre.

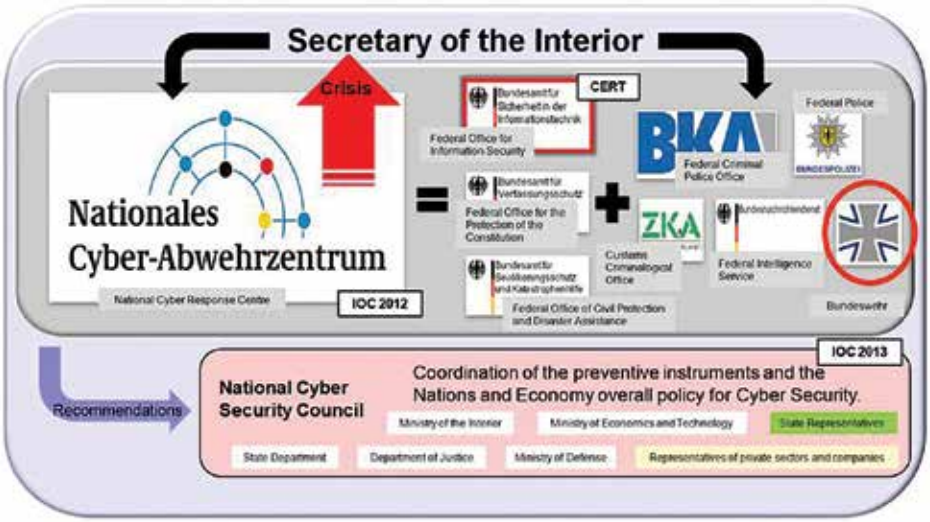



**Figure 5 (Comprehensive) National Cyber Security Architecture**

The National Cyber Response Centre established by the Federal Ministry of the Interior is the pivotal point for the cooperation of all government agencies as well as for the coordination of protective and counter-measures in case of IT incidents. The BSI, the Federal Office of Civil Protection and Disaster Assistance, the Federal Office for the Protection of the Constitution, the Federal Intelligence Service, the Federal Criminal Police Office, the Customs Criminological Office, the Federal Police and the Bundeswehr participate in these measures in the framework of their constitutional and legal guidelines. Agencies representing the Bundeswehr are the Federal Office of Bundeswehr Equipment, Information Technology and In-Service Support and the Military Counterintelligence Service as well as the Bundeswehr IT System Center.

At the international level, Germany is represented in the NATO Cooperative Cyber Defence Centre of Excellence in Tallinn Estonia (See Figure 5 above).

## Structures and Capabilities of the Bundeswehr

In contrast to the U.S. approach, Bundeswehr assets and capabilities in the fields of intelligence, surveillance and reconnaissance, CIS, Electronic Warfare, IT security and Cyber Network Operations are already joint, but organized in separate structures.

• The IT Director at the German Federal Ministry of Defense is the Bundeswehr's IT Security Officer and has technical-organizational responsibility for IT security.

His deputy is the Deputy Director of the Federal Office of Bundeswehr Equipment, Information Technology and In-Service Support.

•The Bundeswehr's Computer Emergency Response Team is subordinate to the Federal Office of Bundeswehr Equipment, Information Technology and In-Service Support; it cooperates closely with the BSI.

•The CERTBw constantly analyzes and assesses the threat situation of the Bundeswehr IT System both for administrative IT (in close coordination with CERT BWI) and IT systems used on operations abroad. Together with other national and international CERT organizations and with the help of its technological sensors, it maintains an up-to-date situation picture of IT security. The CERT Bw and the CERT BWI are the central IT security monitoring authorities of the Bundeswehr IT System.

•The Bundeswehr Communication and Information Systems Command has overall responsibility for use and operation of the Bundeswehr IT System and it may activate a Bundeswehr Risk Management Board whenever an acute crisis emerges. In the context of Cyber/Computer Network Defense, this Board coordinates measures to prevent (further) attacks aimed at IT systems and to restore IT security.

•The BITS of the Bundeswehr Communications and Information Systems Command maintains a current overall situation picture of the Bundeswehr IT System, but also looks at non-IT threats (e.g. natural disasters.

•The Bundeswehr's Strategic Reconnaissance Command exercises command and control over the assets earmarked to conduct Cyber/ Computer Network Exploitation, Cyber/ Computer Network Attack and EW. These forces are tasked with supporting military operations by executing reconnaissance and effects measures (See Figure 6 below).

## Assessment

In implementing its Cyber Security Strategy, Germany appears to be well prepared with regard to countering future threats to Cyber security. Existing Cyber capabilities and those currently being developed deliberately remain the

**(Continued on page 34)**

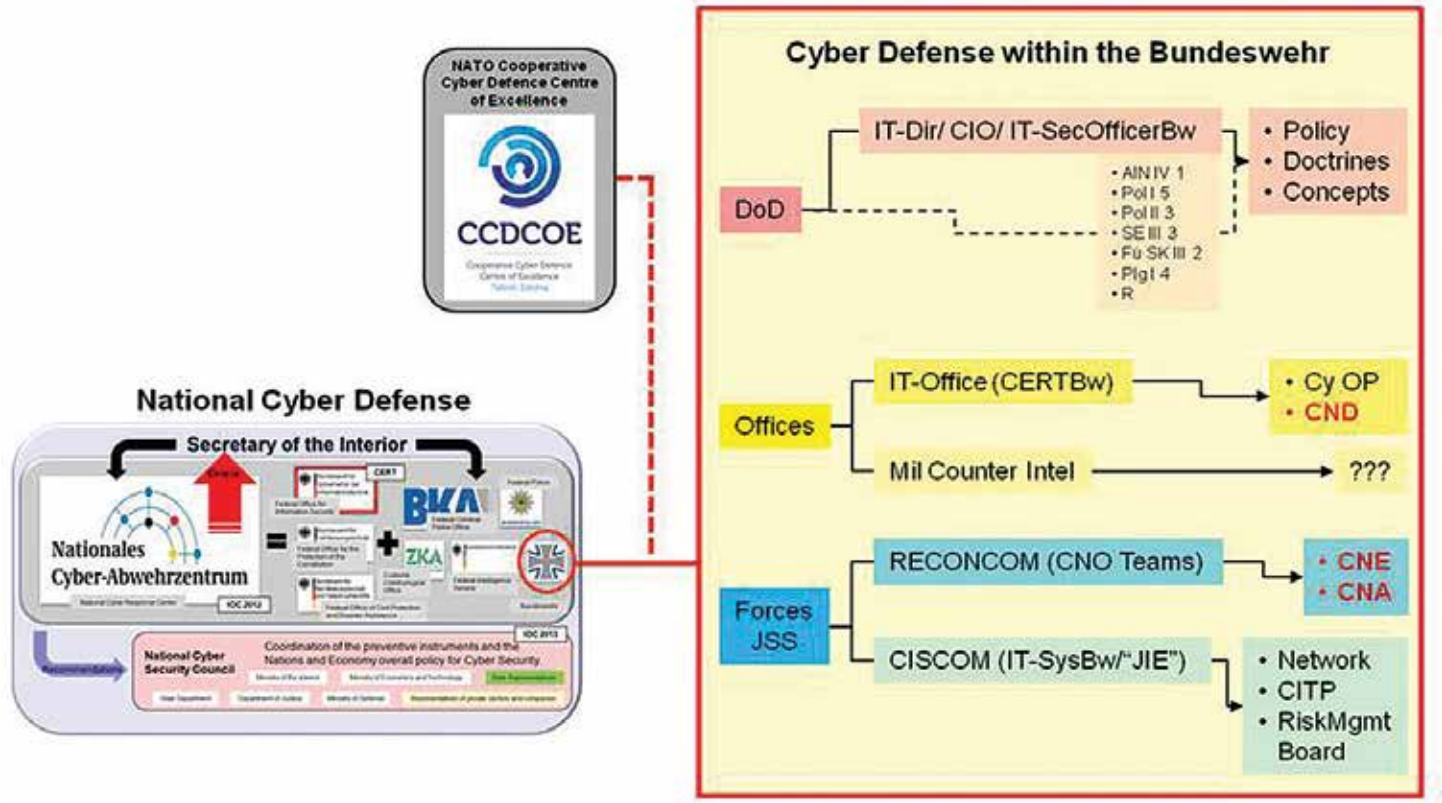



**Figure 6 Cyber Tasks and Responsibilities of the Bundeswehr**

(Continued from page 33)

responsibility of the respective ministries and are being coordinated in the NCRC. Similar to the U.S. approach, the German Government in its Cyber Report underscores the increasing importance of the Cyber Domain for the Bundeswehr. It particularly points out the necessity and legitimacy of 'targeted and coordinated measures of the Armed Forces aimed at impairing adversary information and communication systems,' while stating that 'this capability has not yet been employed.'

The U.S. Army consistently combines its Cyber forces under unified command, complements its capabilities by offensive measures and synchronizes these as an integral part of the conduct of operations in missions abroad and, in addition, realizes newly structured and overarching training (CIS, Cyber, EW). In comparison, the organizational and procedural approach of the Bundeswehr with its currently established distribution of competences and many individual responsibilities appears to be complex and, considering future challenges, purposeful only to a limited extent.

•The various assets working in the electromagnetic spectrum are organized separately in the Bundeswehr. This requires a considerable number of technical interfaces on the one hand and calls for solutions that make these forces efficiently available to the commander on the other. For this, however, the Bundeswehr currently neither has a command structure comparable to the U.S. ARCYBER nor (proven) ideas, concepts and procedures.

•From a technological point of view, comprehensive protection requires an understanding of the entire Bundeswehr IT System all the way through to its operations-related elements used in mobile communications. In reality, however, several IT and Cyber situation pictures are being maintained and updated by different responsible agencies, and Cyber personnel is trained in separate training programs.

•Currently, the training, advanced training, and sensitization of military leaders does not come up to the importance of "Cyber as a new domain." Much less do they appear suitable for recognizing the threats emanating from it and utilizing the opportunities resulting from controlling it.

•So far, respective Bundeswehr units and agencies have not been cooperating with those of the U.S. military in the field of Cyber operations. Besides missing out on information, the opportunity to start/attempt trustful cooperation in this currently highly charged area is thus not exploited.

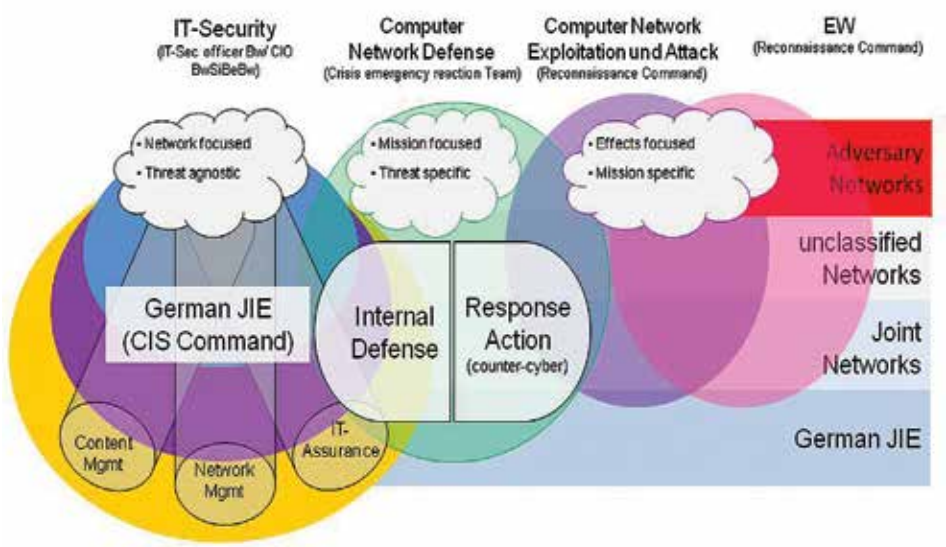



**Figure 7 Technological and organizational complexity in the electromagnetic spectrum**

## The logical chain of "Personnel follows Organization follows Mission follows Concept"

Using this principle, we have to ask the following questions in the field of Cyber:

"What overarching measures are required regarding concepts, organization, joint/coordinated training, national and international cooperation and (technological) materiel and equipment?"

"How can a Cyber capability package for an operation commander be

efficiently provided from the subcapabilities of CERT, CNA, IT security, military intelligence, EW, CIS support and information operations?"

"How can Computer/ Cyber Network Operations be adequately integrated and synchronized in operations planning, and portrayed in a common Cyber Operational picture?" (See Figure 7 on page 34).

## Need for Action

Especially from the operational viewpoint, but also to improve efficiency (avoidance of effort duplication and technological interfaces) and make own capabilities transparent, the following fields of action for improving the effectiveness of military operations emerge for German military units and agencies tasked with Cyber activities.

•In the short term, it appears to be sensible to evaluate the new U.S. Cyber concepts and doctrines, to get relevant and purposeful reports from the German liaison organization in the U.S., to exchange information through visits to the U.S. (Joint) Cyber Command, U.S. ARCYBER and Cyber CoE and, after analyzing further information requirements, the utilization of official requests for information.

•In the medium term, following the British and French example, a permanent German presence in all U.S. Cyber units and agencies appears to be advisable. In addition, the coordination of the training of IT security, CIS, and CNO personnel should be carried out under single responsibility, possibly by merging the training efforts.

•In the long term, it would seem appropriate to review the organizational structure of all German military agencies currently tasked with Cyber activities. For organizational, technical and financial reasons, but also from the operational viewpoint, the central, comprehensive provision of Cyber capabilities (command structure, concepts, personnel and materiel) appears to be an appropriate solution. Establishing a Cyber capability command would be one option; merging all Cyber capabilities in one already existing capability coordination command is another option. This also includes complementing the currently mostly defensive orientation of German Cyber capabilities on operations with specifically defined offensive measures, making centrally provided Cyber Teams integral parts of operations planning.

***Lieutenant Colonel Frank Beyer*** *is the Head of the German Liaision Team to the U.S. Army Cyber Center of Excellence headquartered in Fort Gordon, Ga., USA.*

## ACRONYM QuickScan

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

**ARCYBER -** U.S. Army Cyber Command
**BAAINBw** - Federal Office of Bundeswehr Equipment, Information Technology and In-Service Support
**BKA** - Federal Criminal Police Office
**BND** - Federal Intelligence Service
**BITS** - Bundeswehr IT System Center
**BSI** - Federal Office for Information Security
**CCD COE** - NATO Cooperative Cyber Defence Centre of Excellence
**CEMA** - Cyber Electromagnetic Activities
**CERT Bw** - Bundeswehr's Computer Emergency Response Team
**CNA** - Cyber/Computer Network Attack
**CNE** - Cyber/Computer Network Exploitation
**CND** - Cyber/Computer Network Defense
**CNO** - Cyber Network Operations
**CIS** - Communications and Information Systems
**Cyber CoE** - U.S. Army Cyber Center of Excellence
**DoD** - Department of Defense
**EW** - Electronic Warfare
**FOC** - Full Operational Capability
**ISR** - Intelligence, Surveillance and Reconnaissance
**IOC** - Initial Operational Capability
**MAD** - Military Counterintelligence Service
**NCRC** - National Cyber Response Centre
**NSA** - National Security Agency
**USASCoE** - U.S. Army Signal Center of Excellence
**ZKA** - Customs Criminological Office

# Reclassifed 25F Soldiers negotiating changing career requirements

*By SFC Matthew M. Peterson*

A significant evolution within the Signal Regiment impacting former enlisted Military Occupational Specialty 25F Soldiers was the elimination of their MOS effective 1 October 2013/ FY14.

Soldiers who were formerly classified MOS 25F and reclassified to MOS 25N on or after 1 April 2013 need to fully understand they are not considered fully qualified if they are also coded with transition Additional Skill Identifier Y2. Soldiers with this designation must complete additional training.

This Y2 ASI does not prevent a Soldier from reenlistment or promotion opportunities at this time. However, the Y2 ASI will impact your unit's readiness. Y2 ASI indicates the Soldier lacks significant training that can move the unit from "circuit based switching" to "IP based switching" skills necessary to fully operate the WIN-T systems.

If you currently have the Y2 ASI, do not be discouraged because there are several methods available for you to become fully qualified and have the transitional ASI Y2 removed.

The methods are as follows:

1. Successful completion of the WIN-T Increment 1 new equipment training course (Titled "WIN-T INC 1 Operator & Maintainer Training") at your unit of assignment. This is conducted by the program manager new equipment training team.
2. Successful completion of the WIN-T Increment 2, 400-hour, new equipment training course (Titled "Tactical Communications Node") at your unit of assignment. This is conducted by the PM NETT.
3. Successful completion of the institutional MOS 25NY2 transition course (260-25NY2 (T) (CT) (Nodal Network Systems Operator Maintainer Y2 Transition Training"). This is conducted at the U.S. Army Signal School, Fort Gordon, Ga.

The following information pertains specifically to the Advance Leader Course. Soldiers who have previously completed MOS 25F ALC prior to 1 Oct 2012 will not be required to attend ALC as a 25N; but must attend the MOS 25NY2 transition course if they have not already received WIN-T Inc 1 or Inc 2 NET. Soldiers with successful completion of the MOS 25F ALC, 260-25F30-45 (Network Switching or Systems Operator-Maintainer ALC), between1 OCT 2012 and 30 SEP 2013, and Soldiers with successful completion of the MOS 25N ALC thereafter, qualify for award of MOS 25N without ASI Y2.

There was a small glitch for Soldiers that have attended the 260-31F10 (CT) (F) course not being able to enroll in the transition course 260-25NY2 (T) (CT) within the Army Training Requirements and Resources System prerequisites. This has been addressed and fixed in ATRRS and qualifying Soldiers can now enroll.

Any Soldier that has successfully completed any of the training methods but still has ASI Y2 on their Enlisted Records Brief may contact the Office Chief of Signal, 25N/25E career manager, SFC Matthew Peterson, at matthew.m.peterson4.mil@mail.mil; DSN 780-8192 or commercial 706-791-8192 for information on getting it removed.

The transition course 260-25NY2 (T) (CT) is fully Headquarters Department of the Army funded for Temporary Duty and return or TDY enroute attendance. Soldiers currently assigned to a unit must see their appropriate schools noncommissioned officer to be scheduled for a class. Soldiers on assignment orders to a new unit assignment need to contact HRC PDNCO, SFC Jonathan Muse, at jonathan.k.muse.mil@mail.mil or commercial 502-613-5448 to get scheduled for class enroute.

Unit leaders are encouraged to ensure your NCO support channel is fully engaged

in getting your Soldiers to the training they need to perform to their maximum potential. You can acquire this and further information at the Office Chief of Signal, Enlisted Division website (https://www.us.army.mil/suite/page/838).

***SFC Matthew M. Peterson*** *is a Signal senior NCO presently serving as the 25N/25E career manager in the Office Chief of Signal. He has served in the U.S. Army for more than 20 years as a Signal NCO. He has previously served as a detachment sergeant, platoon sergeant and S6 NCOIC.*

## ACRONYM QuickScan

**ATTRS** - Army Training Requirements and Resources System
**ASI** - Additional Skill Identifier
**ALC** - Advance Leader Course
**ERB** - Enlisted Records Brief
**MOS** - Military Occupational Specialty
**NCO** - Noncommissioned Officer
**NCOIC -** Noncommissioned Officer in Charge
**NET** - new equipment training
**PM** - Program Manager
**NETT** - new equipment training team
**TCN** - Tactical Communications Node
**TDY** - Temporary Duty

# Statement of Ownership, Management and Circulation

UNITED STATES POSTAL SERVICE

**Statement of Ownership, Management, and Circulation (Requester Publications Only)**

| | | |
|---|---|---|
| 1. Publication Title: ARMY COMMUNICATOR | 2. Publication Number: 3 0 5 - 4 7 0 | 3. Filing Date: 1 OCT 2014 |
| 4. Issue Frequency: QUARTERLY | 5. Number of Issues Published Annually: FOUR (4) | 6. Annual Subscription Price (If any): $0 |

7. Complete Mailing Address of Known Office of Publication (Not printer) (Street, city, county, state, and ZIP+4®): ARMY CYBER CENTER OF EXCELLENCE, 513 CHAMBERLAIN AVE BLDG 29808A FT. GORDON, (RICHMOND CTY), GA 30905-5301 — Contact Person: LARRY EDMOND; Telephone (Include area code): (706) 791-7204

8. Complete Mailing Address of Headquarters or General Business Office of Publisher (Not printer): CHIEF OF SIGNAL, U.S. ARMY CYBER 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): TODD BOUDREAU, OCOS DIRECTOR, U.S. ARMY CYBER CENTER OF EXCELLENCE, 513 CHAMBERLAIN AVEBLDG 29808A, RM 713, FT. GORDON, (RICHMOND CTY), GA 30905-5301

Editor (Name and complete mailing address): LARRY EDMOND, U.S. ARMY CYBER 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-R, July 2014 (Page 1 of 4 (See instructions page 4)) PSN: 7530-09-000-9931 PRIVACY NOTICE: See our privacy policy on www.usps.com.

| 13. Publication Title: ARMY COMMUNICATOR | | | 14. Issue Date for Circulation Data Below: FALL SEPTEMBER 2014 | |
|---|---|---|---|---|
| 15. Extent and Nature of Circulation: U.S. ARMED FORCES--CONUS | | | Average No. Copies Each Issue During Preceding 12 Months | No. Copies of Single Issue Published Nearest to Filing Date |
| a. Total Number of Copies (Net press run) | | | 5,500 | 5,400 |
| b. Legitimate Paid and/or Requested Distribution (By mail and outside the mail) | (1) | Outside County Paid/Requested Mail Subscriptions stated on PS Form 3541. (Include direct written request from recipient, telemarketing, and Internet requests from recipient, paid subscriptions including nominal rate subscriptions, employer requests, advertiser's proof copies, and exchange copies.) | NONE | NONE |
| | (2) | In-County Paid/Requested Mail Subscriptions stated on PS Form 3541. (Include direct written request from recipient, telemarketing, and Internet requests from recipient, paid subscriptions including nominal rate subscriptions, employer requests, advertiser's proof copies, and exchange copies.) | NONE | NONE |
| | (3) | Sales Through Dealers and Carriers, Street Vendors, Counter Sales, and Other Paid or Requested Distribution Outside USPS® | NONE | NONE |
| | (4) | Requested Copies Distributed by Other Mail Classes Through the USPS (e.g., First-Class Mail®) | 4,571 | 4,830 |
| c. Total Paid and/or Requested Circulation (Sum of 15b (1), (2), (3), and (4)) ▶ | | | 4,571 | 4,830 |
| d. Nonrequested Distribution (By mail and outside the mail) | (1) | Outside County Nonrequested Copies Stated on PS Form 3541 (include sample copies, requests over 3 years old, requests induced by a premium, bulk sales and requests including association requests, names obtained from business directories, lists, and other sources) | 100 | 100 |
| | (2) | In-County Nonrequested Copies Stated on PS Form 3541 (include sample copies, requests over 3 years old, requests induced by a premium, bulk sales and requests including association requests, names obtained from business directories, lists, and other sources) | 50 | 50 |
| | (3) | Nonrequested Copies Distributed Through the USPS by Other Classes of Mail (e.g., First-Class Mail, nonrequestor copies mailed in excess of 10% limit mailed at Standard Mail® or Package Services rates) | 10 | 10 |
| | (4) | Nonrequested Copies Distributed Outside the Mail (include pickup stands, trade shows, showrooms, and other sources) | 300 | 300 |
| e. Total Nonrequested Distribution (Sum of 15d (1), (2), (3) and (4)) | | | 460 | 460 |
| f. Total Distribution (Sum of 15c and e) ▶ | | | 5,031 | 5,290 |
| g. Copies not Distributed (See instructions to Publishers #4, page #3) ▶ | | | 469 | 110 |
| h. Total (Sum of 15f and g) | | | 5,500 | 5,400 |
| i. Percent Paid and/or Requested Circulation (15c divided by 15f times 100) ▶ | | | 85.7% | 89.4% |

* If you are claiming electronic copies, go to line 16 on page 3. If you are not claiming electronic copies, skip to line 17 on page 3.

UNITED STATES POSTAL SERVICE

**Statement of Ownership, Management, and Circulation (Requester Publications Only)**

| 16. Electronic Copy Circulation | Average No. Copies Each Issue During Previous 12 Months | No. Copies of Single Issue Published Nearest to Filing Date |
|---|---|---|
| a. Requested and Paid Electronic Copies ▶ | -0- | -0- |
| b. Total Requested and Paid Print Copies (Line 15c) + Requested/Paid Electronic Copies (Line 16a) ▶ | 4,571 | 4,830 |
| c. Total Requested Copy Distribution (Line 15f) + Requested/Paid Electronic Copies (Line 16a) ▶ | 5,031 | 5,290 |
| d. Percent Paid and/or Requested Circulation (Both Print & Electronic Copies) (16b divided by 16c × 100) ▶ | 90.9% | 91.3% |

X I certify that 50% of all my distributed copies (electronic and print) are legitimate requests or paid copies.

17. Publication of Statement of Ownership for a Requester Publication is required and will be printed in the WINTER 2014 issue of this publication.

18. Signature and Title of Editor, Publisher, Business Manager, or Owner: Larry Edmond — LARRY EDMOND, EDITOR — Date: 24 SEPT 2014

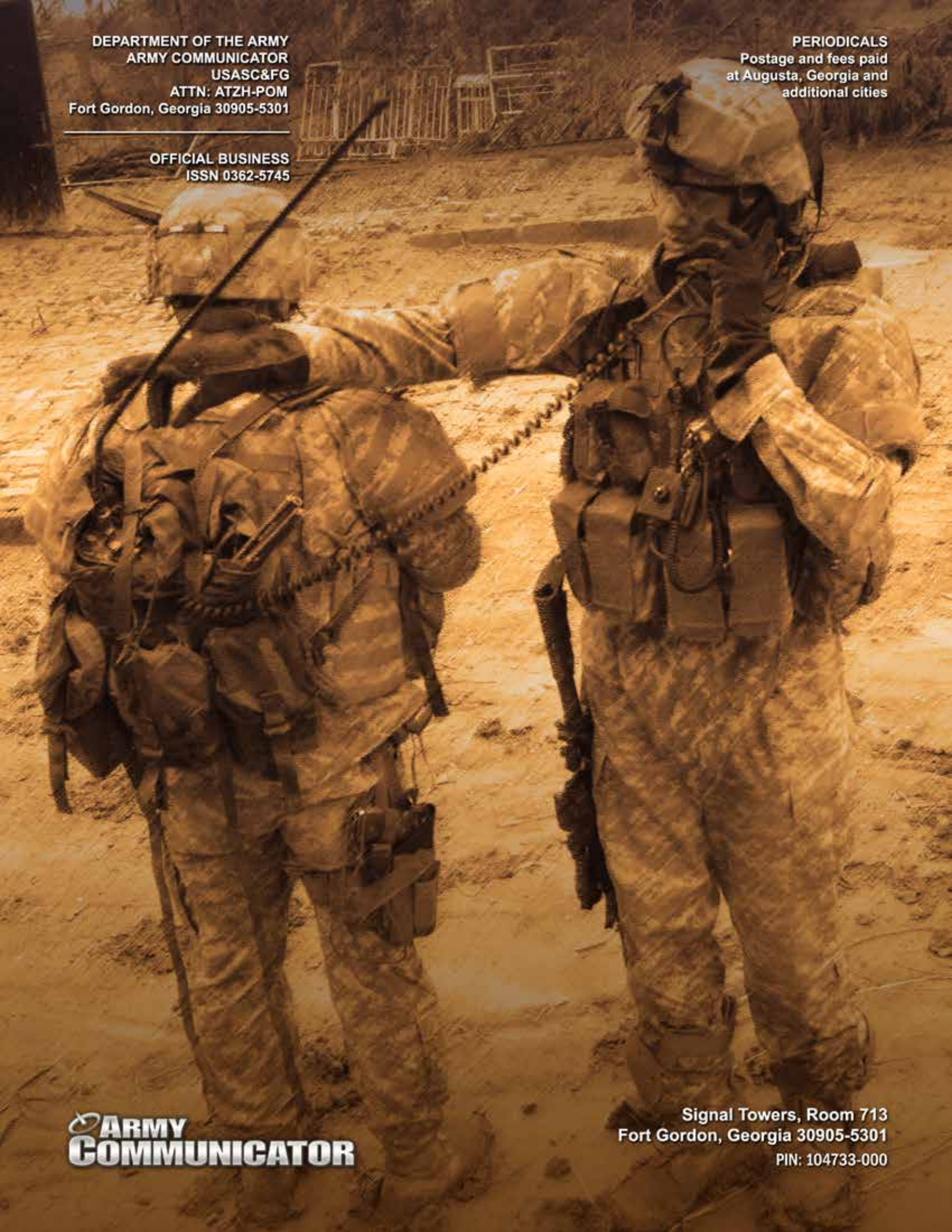
I certify that all information furnished on this form is true and complete. I understand that anyone who furnishes false or misleading information on this form or who omits material or information requested on the form may be subject to criminal sanctions (including fines and imprisonment) and/or civil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

***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.**

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

OFFICIAL BUSINESS
ISSN 0362-5745

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



# ARMY COMMUNICATOR

Signal Towers, Room 713
Fort Gordon, Georgia 30905-5301
PIN: 104733-000