

ARMY COMMUNICATOR

Voice of the Signal Regiment

PB 11-14-1 2013 Vol. 39 No. 1

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

SIGNAL/CYBER

TRANSFORMATION

Meeting the Challenges of Cyberspace Domination

PASSWORD

PLUS:

- *Fort Gordon named home to Cyber Center of Excellence*
- *Army Chief of Staff talks Cyber*
- *What's in store for the Force of 2025 & Beyond*

Signal Regiment still leading the way

Signaleers,

On 28 March 2014, the U.S. Army Signal Center of Excellence at Fort Gordon, was renamed the U.S. Army Cyber Center of Excellence.

The quiet ceremony, with over 150 guests and local civic leaders on hand, belied the significance of the event—a recognition of the increasing importance of cyberwarfare in our Profession of Arms. The ability to exploit the digital domain will usher in a new form of warfare—and the Signal Regiment is already at the leading edge of this shift.

As the Army winds down from two large-scale wars overseas, it is facing a fiscal climate that is forcing it to reevaluate its priorities. Our manpower is shrinking along with our budgets. This new era of reduced manpower and shrinking budgets calls for a new strategy, and senior Army leaders have delivered. Joining with our Marine Corps and Special Operations partners, the Army is exploring the concept of Strategic Landpower—namely, how the elements of landpower can be best employed to support national strategic objectives. Central to this concept is the confluence of land, human, and

“This historic transition to the Cyber Center of Excellence is reminiscent of another one that occurred 151 years ago...”

cyberspace domains in pursuit of those objectives.

The very fact that senior leaders across three disparate sections of our Armed Forces place cyberspace on equal footing with the land domain and newly-developed human domain, reveals the truly important nature of our signal and cyber missions. Just as land can be seized and exploited, and human populations engaged and influenced, cyberspace is a domain that can be dominated to prevent its use by an adversary.

And that is the focus of both the Cyber Center of Excellence and the Signal Regiment.

Within the Signal Regiment, this paradigm shift has already taken hold. Instead of viewing communications

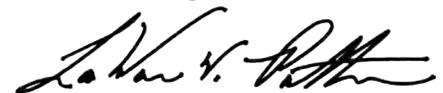
networks as only a means of transporting voice and data, we have increasingly focused on the necessity of securing it from incursions. Recognizing this reality, we have led the way during the last seven years with the development of two new cyber-focused Signal MOSs—255S Information Protection Technician for warrant officers and 25D Cyber Network Defender for non-commissioned officers—both of which are presently in high demand!

As the Cyber Center of Excellence, we will take the Army’s Unified Land Operations definition of “seize, retain, and exploit the initiative to gain a position of relative advantage” and apply it to cyberspace and the electromagnetic spectrum. We will still build, operate, and maintain the network—that has not changed. But we will also defend it against emerging threats, taking the fight to the enemy to deny them the use of this key terrain.

This historic transition to the Cyber Center of Excellence is reminiscent of another one that occurred 151 years ago that same month. In March of 1863, President Abraham Lincoln signed legislation authorizing the creation of a permanent Signal Corps.

It is fitting, then, that in March of 2014, the same Signal Corps announced to the world that it had moved into a new era, and that it possesses the tools, professional warriors, and training to win the fight.

Pro Patria Vigilans!



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



COMMAND

Chief of Signal
MG LaWarren V. Patterson

Regimental Chief Warrant Officer
CW5 Peter T. Winter

Regimental Command Sergeant Major
CSM Ronald S. Pflieger

EDITORIAL STAFF

Editor-in-Chief
Larry Edmond

Art Director/Graphic Designer
Billy Cheney

Photography
Billy Cheney, SSG Steve Cortez, Bill Bengston

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 1413301

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

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

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

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

Army Communicator reserves the right to edit material.

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

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

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

ARMY COMMUNICATOR

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

PB 11-14-01
Spring 2014
Vol. 39 No. 1

Voice of the Signal Regiment

Table of Contents

Features

- | | |
|--|---|
| <p>5 Army Chief of Staff discusses cyberspace future
Jennifer Downing</p> <p>6 Signal Center changes to Cyber Center</p> <p>8 New mission integrates related cyberspace operations training
Russell Fenton
David L. Smith</p> <p>11 Cyber Center of Excellence generates new doctrine
LTC Edie M. Fairbank</p> <p>14 Cyberspace training permeates professional military education
MAJ Robert L. Collins III</p> <p>17 Wherefore came this cyber thing?
CW5 Curtis McDonald</p> <p>19 Cyberspace operations impacts landpower
MAJ Irvin Oliver</p> <p>23 Investing to secure the future
Steve Townsend
Dr. Stephen B. Chaney</p> | <p>29 Building the Cyber-Electromagnetic Career field</p> <p>33 Frequently asked questions about the 25D MOS</p> <p>36 Human Resources Command stands up new Cyber Branch
LTC Chevelle Thomas</p> <p>38 Army researchers looking to blend electronic warfare
Kristen Kushiyama</p> <p>41 Joint Readiness Training Center offers broadening assignment
CPT Vasilios Agapios
CPT Chaz Jordan</p> <p>44 44th ESB executing mission
CPT Christina Knight
CPT Sean Ruddy</p> <p>48 New field support model implemented
Richard Licata</p> |
|--|---|

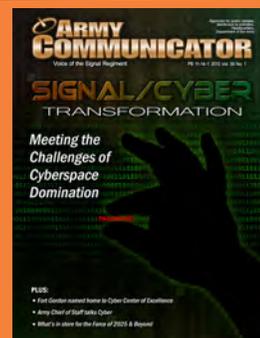
Is the 25D MOS and a COMSEC custodian assignment a one-way ticket to the COMSEC vault...See the answer to this and several other key questions on Page 33.



Join the Discussion

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

Cover: This edition of the *Army Communicator* provides a snapshot of the rapidly changing landscape of the Signal Regiment as the cyberspace operations mission expands. Fort Gordon is designated as the new home for cyberspace operations training.



Cover design by Billy Cheney

Cyber transformation natural response

Signaleers,

The decision to transition the Signal Center of Excellence to the Cyber Center of Excellence seems like the natural evolution. Signal Regiment members have always provided cutting edge innovations for our nation. Our dedication to network defense, in today's vernacular is captured in cyber security.

As threats to cyberspace become more pervasive, leaders throughout the Regiment recognize our responsibilities and are moving proactively to develop qualified experts like those in the new warrant officer MOS—the 255S Information Protection Technician. These highly skilled warrant officers, who we started training back in 2009, have become a highly sought after cyber resource in every echelon of command. Similarly, shortly thereafter, we realized the need for experienced NCOs and we instituted the 25D Cyber Network Defender MOS. Last year, we graduated our first two classes. Another

98

staff sergeants will matriculate through the course in FY14. The 25D MOS will be funded through the POM in 2017.

Cyber trained specialists were originally designated to fill a need within FORSCOM units, enabling commanders to defend their networks while in the tactical environment. However, the demand for the cyber skill set is so high that Cyber Protection Teams within the NETCOM community have the right of first refusal of the 25D graduates. It is expected that NETCOM units will have priority until they are fully staffed. We expect FORSCOM units to begin receiving the Cyber Network Defenders by the end of FY 16.

In order to better address these urgent requirements, we are beginning the work to create a Cyber-series MOSs, 17. This training will be very similar in the core to the 25D program, but will be designed for NETCOM units operating in both the tactical and strategic sides of Cyber. This will allow our 25Ds to either return to their originally intended role, working alongside battalion-and-higher Signal staffs to protect unit tactical networks from cyber threats or convert to the 17 series MOS.

A critical understanding that should be gleaned from the current transitions is that Signal Regiment leaders are fully cognizant of our responsibilities. We have embraced cyber and expect many exciting changes in the immediate and long-term future.

Your Signal Regiment is once again giving birth to a new field of expertise, as it did in the past when it created the Army's meteorological service and aviation service.

Where we will be 20 years from now remains to be seen, but one thing is certain—the Signal Regiment will be as proud and strong as ever!



Cyber role offering great opportunities

Signaleers,

Exciting times are ahead for both the Signal Corps and the U.S. Army!

On 28 March 2014, the U.S. Army Cyber Center of Excellence sign unveiling marked another pivotal change in the history of Signaleers, as our understanding of the network has grown. More than just a means to communicate, we recognize the network as a digital domain, an element of strategic landpower, something that can be held and exploited in ways that we cannot yet imagine.

As your newly installed Regimental Chief Warrant Officer, I am privileged to be a part of the leadership team orchestrating this change. I am eager to continue forging a way ahead for the Signal Regiment, especially our warrant officer cohort

We must all prepare ourselves for a new set of challenges and opportunities. Army leaders are challenged with level-setting in order to remain responsive and relevant while at the same time, implementing Congressionally mandated cutbacks. As a result we can expect continuing cutbacks throughout the force.

This does not mean that all is doom and gloom. We Signaleers are positioned in the midst of a growth industry.

The Army is more dependent

than ever upon its network, and the urgency of cyber defense is shining a spotlight on the professionalism and expertise of our Regiment, as we lead the way into this evolving domain. As the newly formed Cyber Protection Brigade and smaller Cyber Protection Teams are coming on line, we require smart, adaptive leader-communicators who must be able to think creatively to solve problems.

We are trying to build the airplane and fly it at the same time--no text books or historical examples are being followed. While scary at times, this also provides us with a great opportunity—the chance to step back, take a look at the bigger picture, and start building it the right way. In order to do so, however, the Signal Regiment needs everyone to pitch in and help.

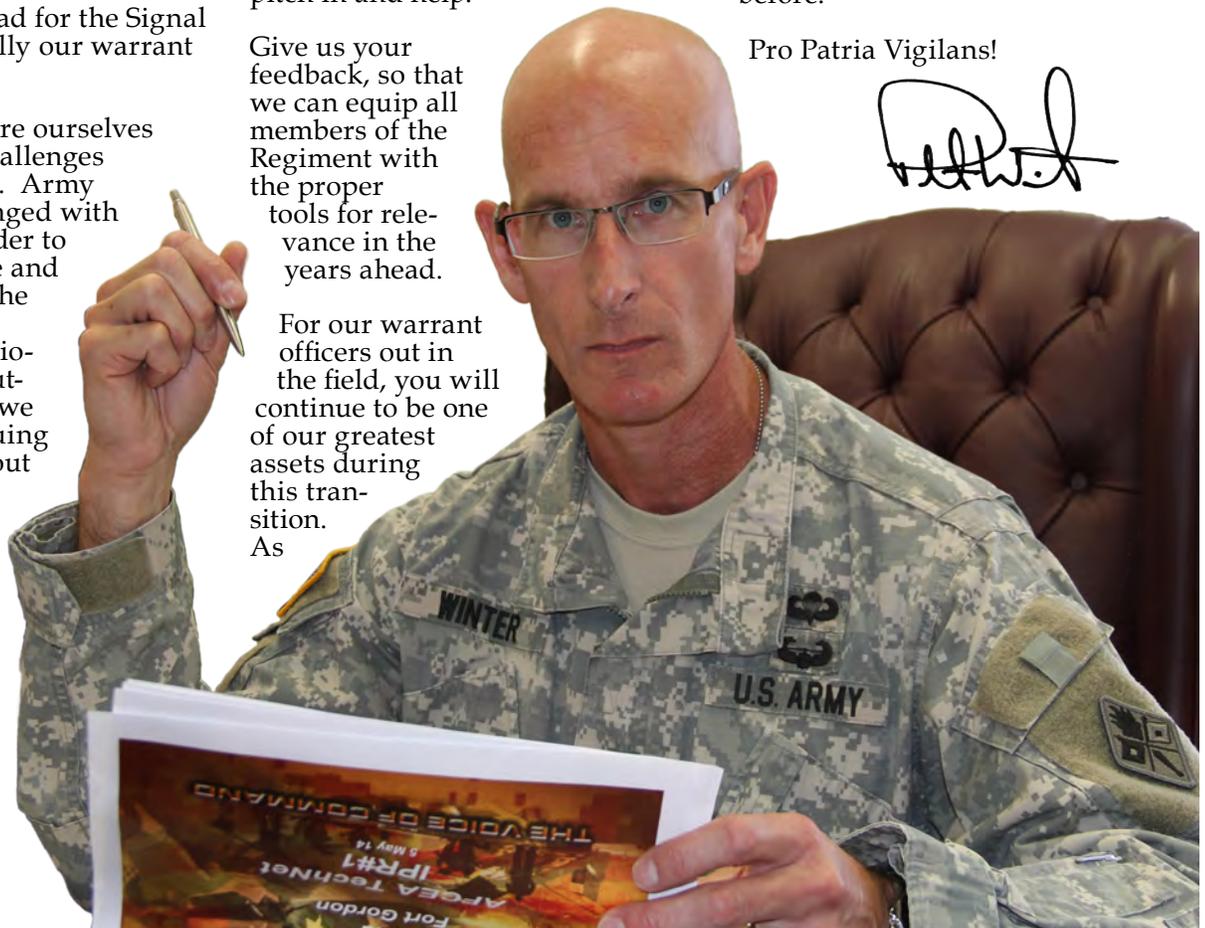
Give us your feedback, so that we can equip all members of the Regiment with the proper tools for relevance in the years ahead.

For our warrant officers out in the field, you will continue to be one of our greatest assets during this transition. As

technicians, you remain the linchpins in the operation and defense of complex information technology systems and networks at all echelons. Aggressively seek ways to improve your “network fighting” position, ensuring systems and networks are properly designed, engineered, configured and patched. Perfect your craft and stay technically relevant. Challenge yourself with assignments that focus creative and critical thinking on unique issues.

For everyone, stay vigilant! Much is at stake, and each of you is a significant protector of the Cyber domain. We have an historic opportunity in front of us. Let us meet the challenges ahead with the professionalism and excellence we have demonstrated so many times before.

Pro Patria Vigilans!



Signal Regiment members earned cyberspace defense training mission

Signaleers,

There have been many changes following the announcement of the Signal Center of Excellence's transition to the U.S. Army Cyber Center of Excellence. We have a new mission—and with our transformation come new signs, new coins, and new titles. But though the outer trappings change, one thing that will remain constant is the role of the non-commissioned officer in enforcing high standards.

We are entering a new age in which keystrokes can halt nations. The skill sets with which we will equip our cyber warriors are immensely powerful and can be used to great effect—rightly or wrongly. Therefore, it is imperative that the moral fiber of the backbone of our Signal Regiment—our NCOs—be unyielding.

One of my goals as Regimental Command Sergeant Major is to emphasize the Profession of Arms within the Regiment. Our profession is built on trust both from our nation and within our ranks, as we live and fight side-by-side, with honor.

As a Center of Excellence, we have met and exceeded standards set forth by the commander of the U.S. Army Training and Doctrine Command for training and capability development. As the Cyber Center of Excellence, we are the nexus for the integration of cyber warfare into the Army's strategic landpower concept. We have earned the trust of our nation to execute this mission. I am proud of the outstanding way in which the Signal Regiment has handled it thus far.

In order to maintain this trust, however, we must continue to show our professionalism, ensuring that Signaleers of all ranks and MOSs understand the ethical principles that are foundational to our institution. We must give our nation the confidence that those who hold the keys to cyberspace are of the highest character.

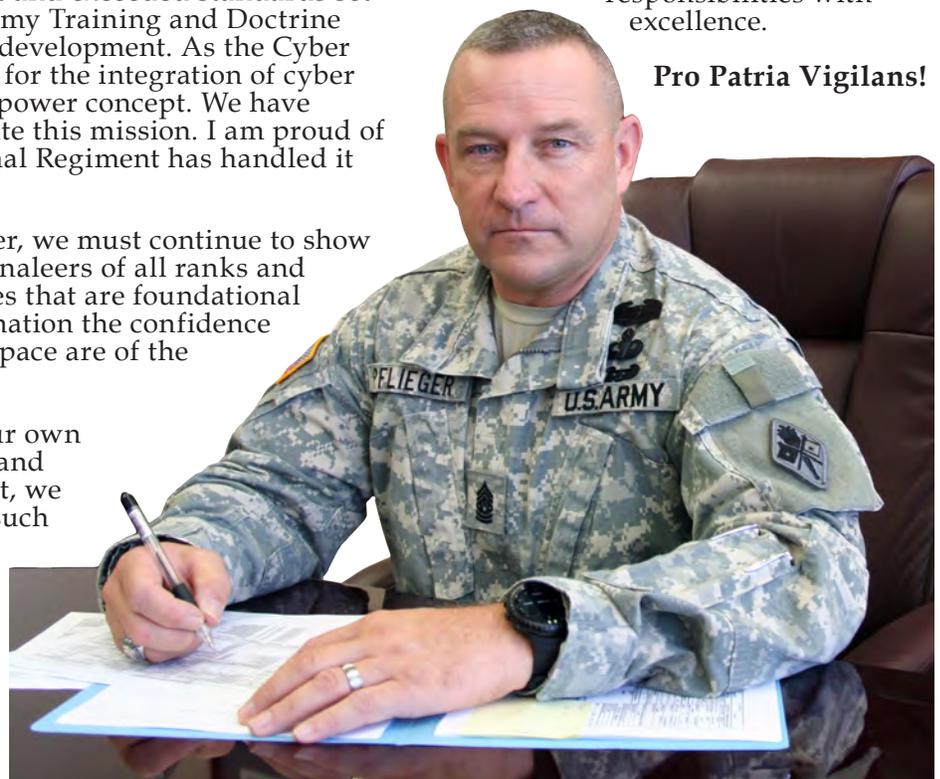
This trust must be first built within our own ranks. By upholding the Army values and maintaining high standards of conduct, we will be able to combat insider threats such as sexual harassment or negligent

discharges of classified information. Our ability to fight our digital battles will only be as strong as the bonds we share within our units.

As we move forward, all members of the Signal Regiment will increasingly find yourselves—and our work in cyberspace—to be in the spotlight. What will be revealed will depend largely on the character and standards we have developed.

I charge all leaders within the Regiment—and especially our NCOs—to demonstrate that we are worthy of the responsibility our Army and nation have placed in our hands. I have the highest confidence in you members of the Signal Regiment to perform your duties and responsibilities with excellence.

Pro Patria Vigilans!



Army Chief of Staff discusses future cyberspace operations



By Jennifer Downing

As cyberspace operations continues to emerge as the new frontier, the Chief of Staff of the Army met with key leaders from U.S. Army Cyber Command to discuss how cyber should be integrated from the tactical to the strategic level of combined arms operations, and recognize employees who continue to work building the command.

GEN Raymond T. Odierno, chief of staff of the Army, visited the headquarters of U.S. Army Cyber Command at Fort Belvoir 22 Jan and met with LTG. Rhett A. Hernandez, commander, U.S Army Cyber Command, and other senior leaders working to build cyber doctrine and those who protect cyber networks daily.

Strong training, leader development, and integration of training and exercises at all levels were prevalent topics of discussion. The chief said the work of Army Cyber is critical to the future of the Army and the way it fights. Army Cyber also plays a key role in the Army's ability to prevent, shape and win with a key mission of incorporating cyber operations into traditional land operations.

"We have to prevent conflict. We need creative and

innovative use of cyber to prevent and shape conflicts," said GEN Odierno. "When you train commanders and staff at all levels, increased understanding of land cyber develops."

Utilizing the skill sets of those serving in the National Guard and Reserves is another way detailed to help meet the



Photo by SSG Steve Cortez

During a visit to U. S. Army Cyber Command on 22 January 2014, GEN Raymond T. Odierno, Chief of Staff of the U.S. Army, took time out of discussing the future of cyberspace operations to award ten Soldiers and civilians with Chief of Staff of the Army Coins of Excellence. GEN Odierno thanked everyone for their dedication and hard work developing cyberspace concepts and mission requirements.

challenge of incorporating cyber across the board. By providing depth across the total force and building capabilities that fully integrate and organize our Reserve partners, the Army can seek skilled personnel and track them as cyber warriors.

The importance of continually linking with U.S. Cyber Command and other partners was also highlighted as an important method of further defining functions and roles.

GEN Odierno described his gratitude to those who "continue to develop an elite cyber force."

"We are just getting started. We are on the verge of a significant high speed revolution.

Over the last two years, the Army has put a lot of great people to work examining every facet of our training, doctrine, and warfighting capability. We did not do this to examine where we stand today.

Rather, all of this effort was aimed at figuring out two things: what kind of Army we will need to meet future challenges, and what we have to do to build that Army even as we continue fighting in Afghanistan and remain engaged throughout the world. Much of what we concluded is available

Proclamation
in recognition
of the
Cyber Center of Excellence

Whereas, Fort Gordon has made an immeasurable contribution to the nation's defense since its establishment in 1941 and,

Whereas, Fort Gordon has graduated generations of skilled military communicators since the Signal Training Corps was established in 1948 and,

Whereas, the U.S. Army Signal Center has played a vital role in the defense of our nation since its designation in 1974 and,

Whereas, cyberspace operations have become a critical challenge that our nation's warriors must meet and,

Whereas, the U. S. Army is transforming the Signal Center of Excellence into the Cyber Center of Excellence to prepare our military personnel to meet challenges in cyberspace and,

Whereas, the Cyber Center of Excellence will lead the continuing essential training of our Signal regiment warriors in addition to the new evolving training and development of our cyber Soldiers and,

Whereas, the Cyber Center of Excellence and other transformation at Fort Gordon will bring thousands of new military personnel, civilian employees and their families to our region and,

Whereas, the city of Augusta and the entire Central Savannah River Area stand proudly in support of the military personnel and families who sacrifice so much to defend our nation's freedoms at Fort Gordon,

Now therefore, I, Deke Copenhaver, Mayor of the city of Augusta, do hereby proclaim March 28, 2014, as Cyber Command of Excellence Day at Augusta, Georgia, in recognition of the ribbon cutting ceremony and urge all citizens to applaud the extraordinary efforts and achievements of the U.S. Army, military personnel, and civilian employees.

Augusta
GEORGIA

- The Honorable Deke Copenhaver
Mayor
Augusta, Georgia

Signal Center changes to Cyber Center

The U.S. Army Signal Center of Excellence became the Cyber Center of Excellence during a ceremony before a crowd of local military and community leaders at Fort Gordon's Gate 1 on 28 March.

MG LaWarren V. Patterson, U.S. Army Cyber Center of Excellence and Fort Gordon commanding general, and Augusta Mayor Deke Copenhaver, unveiled a new sign that marks the installation as home to the Army's cyber warriors.

MG Patterson will command the Cyber Center of Excellence, which will oversee both signal and cyber training. The Cyber Center will concentrate on doctrine, organization, training, materiel, leadership, personnel and facilities for signal and cyber Soldiers.

Prior to the unveiling, Copenhaver addressed the crowd by saying, "To Fort Gordon and to our military I want to say thank you for making this exciting day possible. I know that we'll see growth in the future but I want to say - more so than anything - thank you and I have a proclamation deliver."

Following Copenhaver's comments and delivery of the proclamation Patterson addressed the crowd.

"Today is a day that has been long in coming," said MG Patterson. "It is with great pleasure and pride



Photo by Bill Bengtson/Fort Gordon Public Affairs Office

MG LaWarren Patterson, U.S. Army Cyber Center of Excellence and Fort Gordon commanding general, responds to media questions after the unveiling of a new welcome sign at Gate 1.

that I welcome you all to the U.S. Army Cyber Center of Excellence and Fort Gordon.

"March is a month that has special significance to the Signal Corps," he said. "One hundred and fifty one years ago this month President Abraham Lincoln signed legislation authorizing the creation of a permanent Signal Corps."

The initial corps was no more than a colonel assisted by two clerks but as MG Patterson shared with the crowd, the corps has grown significantly since that time.

"Our information age has witnessed an exponential increase in the capabilities of our networks," said MG

Patterson. "This has led to a surge in the number of attempts to exploit that network infrastructure upon which our global community so heavily depends and with our increasing data-reliant Army it is clear that protecting cyber space is vital to the basic Signal mission of providing reliable networks to enable mission command. Transformation of the Signal Center of Excellence to the Cyber Center of excellence is a crucial step in recognizing this new reality. It demonstrates our affirmation that cyber space is a domain which we can seize and utilize as an element of strategic land power."

New mission integrates related cyberspace operations training

By Russell Fenton and David L. Smith

Army leaders recently took a huge step into the future by designating Fort Gordon as the Cyber Center of Excellence.

This step highlights an understanding of the importance electromagnetic spectrum management and cyberspace dominance. Additionally this move is designed to posture the force for success in future operations.

For Fort Gordon, this marks the beginning of a transformation that will continue over the next several years as the post becomes a primary focal point for Army and Department of Defense cyberspace operations.

The process for selecting Fort Gordon as the location for the U.S. Army Cyber Center of Excellence, and more importantly, the decision to transition the Signal Center of Excellence to the Cyber CoE, was not an easy one.

About a year ago, the then SigCoE was informed that GEN Robert Cone, commander of the U.S. Army Training and Doctrine Command, planned to gain Chief of Staff of the Army concurrence for transferring force modernization proponent responsibilities for cyberspace operations from Army Cyber commander to TRADOC in order to achieve institutional unity of effort.

The ARCYBER commander at the time (LTG Rhett Hernandez) supported this effort because it was his desire to focus the command entirely on the operational mission. Subsequently, GEN Cone wanted a recommendation as to which TRADOC organization should receive the mission and transition to a Cyber CoE. This resulted in the SigCoE producing and submitting a plan that described how new roles and responsibilities would be integrated into its current mission and structure. The plan also

provided an understanding of the projected resources required.

The SigCoE plan was selected by TRADOC as the preferred course of action to bring forth for CSA concurrence and on 31 May 2013, the CSA agreed with GEN Cone's proposal and recommendation. The CSA also directed TRADOC to transfer Electronic Warfare FMP responsibilities from the Combined Arms Center at Fort Leavenworth to the Cyber CoE in order to facilitate the development of capabilities that support the convergence of cyberspace and the EMS.

Moreover, the CSA directed the establishment of Signal and Cyber Schools to ensure Soldiers and civilians receive the right training and education necessary to build the technical and tactical knowledge, skills, and abilities necessary to fight in and through cyberspace and the EMS in the 21st century.

Although the CSA concurred with the recommendation, Secretary of the Army approval was still required in order to move forward with the plan; thus the next several months following the CSA's decision were spent gaining additional Army leadership guidance and conducting the necessary analytical work that culminated in the presentation of a business case analysis for final endorsement by the Honorable John McHugh.

On 19 December 2013, approximately eight months after the genesis of GEN Cone's effort to place FMP for cyberspace operations under TRADOC, the Secretary of the Army officially announced that the Army would establish a Cyber CoE at Fort Gordon with the mission to integrate and produce cyberspace operations, Signal/communications networks and information services, and EW related doctrine,

organizational, training, materiel, leadership/education, personnel, and facility solutions that enable commanders and leaders to achieve freedom of action in and through cyberspace and the EMS.

Some may ask, "why the SigCoE and Fort Gordon?"

While Army decision makers did consider other organizations and locations, in an era of limited resources and shrinking budgets, they expressed a need to take advantage of the efficiencies realized by leveraging an existing Center of Excellence structure (the SigCoE) already charged with developing a considerable segment of solutions related to cyberspace and EW.

The Augusta, Ga. area and its low cost-of-living will keep personnel costs to a minimum in comparison with Fort Leavenworth and Fort Meade (the other locations considered). Finally, the National Security Agency and U.S. Cyber Command elements already present on Fort Gordon, along with the stand-up of a Joint Forces Headquarters – Cyber and future move of ARCYBER to the post mean the Army has a unique opportunity to establish an institution at the same location where an increasing level of cyberspace operations will occur.

The possibility for collaboration, once all are situated on Fort Gordon, will be tremendous – another aspect that could not be overlooked

by leadership when making the final decision.

The transition to the CyberCoE will be done in three phases. Provisional status (Phase I) has already begun based on the Secretary of the Army announcement on 19 December 2013. During this time, the SigCoE will be referred to as the Cyber CoE. Command authorities continue to officially reside with the commanding general, SigCoE.

Cyber FMP personnel at Fort Meade and EW FMP personnel at Fort Leavenworth will be under the operational control of the provisional CyberCoE. The provisional organization will begin to serve as the FMP for cyberspace operations, Signal/communications networks and information services, and EW. Finally, the CG will be responsible for the provisioning of Signal, Cyber, and EW Training for the Army. To support the CG in this task, both the provisional Signal and Cyber School Commandants will start to transition the appropriate courses under their oversight. It is important to note that the EW training at Fort Sill and Fort Huachuca will come under the oversight of the Cyber School commandant. Phase I will end upon the approval of concept and station plans that provide a validation and resources to a proposed structure; which is projected to occur by 1 October 14.

Phase II is referred to as the initial operating capability phase and is set to begin

upon the official completion of Phase I tasks. During this time, the CG, Sig CoE becomes CG, Cyber CoE and continues executing FMP responsibilities for cyberspace operations, Signal/communications networks and information services, and EW. Additionally, the CG, Cyber CoE will begin to lead the lifecycle management of Cyber Personnel as part of a Cyber Branch currently in development. Additionally, the Cyber CoE will stand-up a TRADOC Capability Manager Office for Cyber. Phase II will end once selected Cyber and EW FMP positions and personnel at Fort Meade and Fort Leavenworth are assigned (versus OPCON) to the Cyber CoE. This is projected to occur by 1 October 2015.

Finally, Phase III will indicate the Cyber CoE is at full operating capability. The phase begins once the previously mentioned tasks are officially complete and ends upon selected Cyber and EW FMP positions and personnel at Fort Meade and Fort Leavenworth relocating (vs. just assigned) to the CyberCoE. This will occur after 01 Oct 15. During this time, the Cyber CoE continues executing FMP responsibilities for cyberspace operations, Signal/communications networks and information services, and EW. Ultimately during this phase, the Cyber CoE must

(Continued on page 10)

(Continued from page 9)

complete the realignment of the organization, finalize remaining personnel moves and hiring actions, and complete the establishment of Signal and Cyber Schools, while continuing to mature partnerships with appropriate external organizations and agencies.

While 28 March 2014 was a great day for the Army, and hopefully the nation, it was just the beginning of a multi-year plan to transition Fort Gordon into one of the key installations supporting Army and DoD cyberspace operations. The intensive work leading to a decision that assigns FMP responsibilities for cyber operations, Signal/communication networks and information services, and EW to a new Cyber CoE borne out of the previous SigCoE has been done and the green light has been given. Now it is time to execute.

The three-phase transition is expected to evolve over several years. The work to come will not be any less arduous than that which was done to obtain a decision. In fact, with the expected impact to personnel and facilities, it will

be more so to mitigate any issues throughout the process. Once full operating capability of the Cyber CoE is reached, the Army should be better postured to provision the right solutions that provide commanders and leaders the ability to achieve freedom of action in cyberspace and the EMS, while denying the enemy the same.

***Russell Fenton** is a Telecommunications Specialist. He presently works as Department of the Army civilian as the chief of the Cyber Cell, TRADOC Capabilities Management Office Global Network Enterprise, U.S. Army Signal Center of Excellence at Fort Gordon, Ga. He is a retired Signal and information systems management (FA53) officer with over 26 years of combined service.*

***David L. Smith** is a senior cyber network Analyst at TRADOC Capability Manager, Global Network Enterprise. He began his military career as a private in the Army Signal Corps in 1986 and retired as a chief warrant officer 4 in 2012. He served 25 years on active duty in Germany, Korea, Bosnia, Iraq and several stateside tours.*

ACRONYM QuickScan

ARCYBER - U S Army Cyber Command
ARNG - Army National Guard
CG - Commanding General
CIO - Chief Information Officer
CoE - Center of Excellence
CONOPS - Concept of Operations
CSA - Chief of Staff of the Army
DA - Department of the Army
DCO - Defensive Cyber Operations
DoD - Department of

Defense
DoDIN - Department of Defense Information Networks
DOTMLPF- Doctrine, Organization, Training, Materiel, Leadership, Personnel, Facility
EMS- Electromagnetic Spectrum
EW- Electronic Warfare
FMP- Force Modernization Proponency
FOC - Full Operating Capability
IER - Information Exchange Requirements

IOC - Initial Operating Capability
JIE - Joint Information Environment
LWN - LandWarNet
NetOps - Network Operations
OCO - Offensive Cyber Operations
OPCON- Operational Control
TCM GNE - TRADOC Capability Manager for Global Network Enterprise
TRADOC- U. S. Army Training and Doctrine Command

Cyber Center of Excellence generates need for new doctrine

By LTC Edie M. Fairbank

As the Signal Center of Excellence transitions into the Cyber Center of Excellence, force modernization proponent responsibilities for cyberspace operations, signal and communications networks and information services, and electronic warfare consolidate under one command.

This consolidation brings new doctrine to the Cyber CoE; Field manual 3-12, Cyberspace Operations, FM 3-38, Cyber Electromagnetic Activities, and Army techniques publication 3-36, Electronic Warfare Techniques.

Combined with the current and developing Signal doctrine, the new cyber doctrine will support the training and operations of a highly-skilled cyber force, trained to joint standards and ready to meet combatant commanders' current and future force requirements. Relevant cyber doctrine will ensure that Army leaders are equipping the force to operate successfully throughout the cyberspace domain and the

electromagnetic spectrum.

Cyberspace is a global domain within the information environment consisting of the interdependent network of information technology infrastructures and resident data, including the Internet, telecommunications network, computer systems, and embedded processors and controllers.

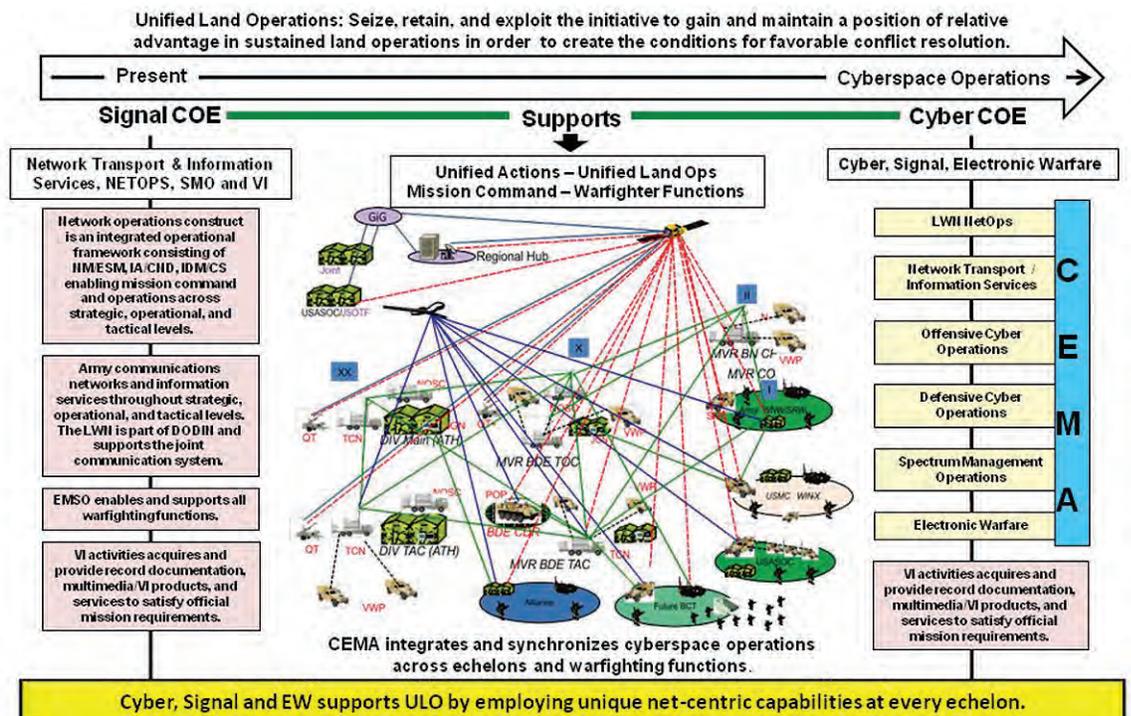
Threats to the conduct of military operations exist in cyberspace resulting in the constant necessity to manage risk and protect portions of cyberspace. Cyber attacks and similar network intrusions or exploitation activities occur throughout cyberspace and result in disruption, neutralization, or exploitation of

data from targeted information technology networks.

Commanders must be aware of these threats and take measures to address them. Effective integration and synchronization of cyberspace operations results in simultaneous and complementary effects leading to achieve objectives consistent with the commander's intent and concept of operations.

FM 3-12 is in initial draft development and provides tactics and procedures for the coordination and integration of cyberspace operations in support of unified land operations. This manual links joint cyberspace operations

(Continued on page 12)



doctrine and ADRP 3-0, Unified Land Operations, providing the methods by which Army forces support and perform offensive cyberspace operations, defensive cyberspace operations, and Department of Defense information network operations, providing opportunities for commanders to integrate specialized cyberspace capabilities in support of their concept of operations. This manual provides an overview of cyberspace and its relationship to the operational environment; examines the roles, responsibilities, and working relationships of joint and Army cyber organizations involved in cyberspace operations; and discusses how cyberspace operations are an integral part of unified land operations. Supporting cyber ATPs are in the planning phase of development.

FM 6-02, Signal Support to Operations, is a new publication that describes the Signal Regiment's roles and responsibilities in support of the Army's mission, commanders, staff officers and signal personnel. It includes three chapters and supporting appendices that address network operations in support of mission command and unified land operations, and the specific tactics and procedures associated with organic and non-organic signal forces providing LandWarNet that enable and support the Army's mission at all echelons across the range of military operations. FM 6-02 is the foundation for nine supporting ATPs that details the techniques regarding the ways and methods to accomplish the missions, functions or tasks of the Signal Corps.

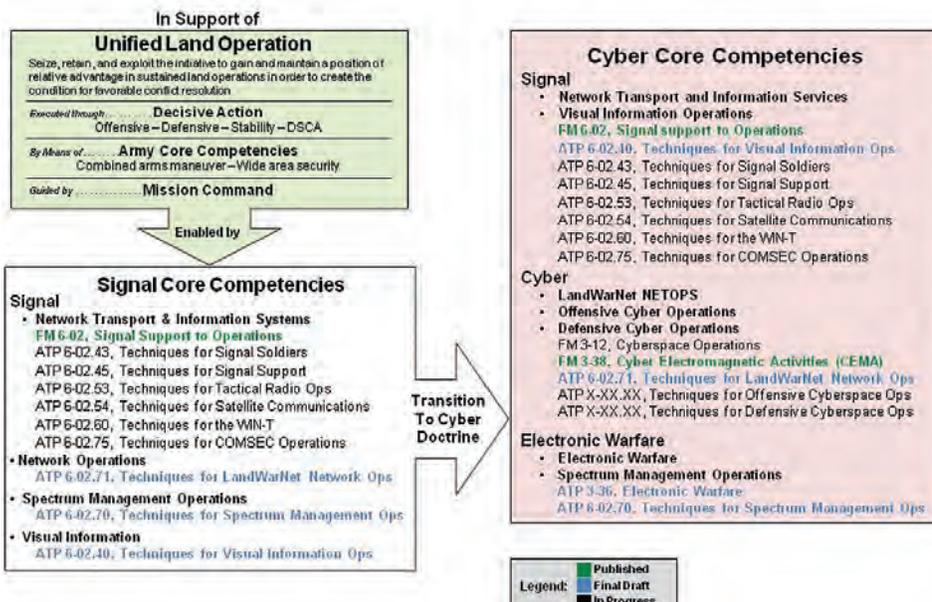
Two Signal ATPs that directly support the cyberspace mission are ATP 6-02.70, Techniques for Spectrum Management Operations, and ATP 6-02.71, Techniques for LandWarNet Network Operations. Both ATPs are in final draft development with expected publication in early 2015.

ATP 6-02.70 provides an overview of SMO and describes how spectrum managers support commanders through the warfighting functions, the military decision making process, and the common operational picture.

It provides technical descriptions of the SMO tool's capabilities as well as use of the tools in executing SMO in unified land operations. ATP 6-02.71 discusses LandWarNet's capabilities as the Army's portion of the Department of Defense information networks and how LandWarNet enables mission command to support unified land operations. Through LandWarNet network operations, the Signal Corps provides the personnel and tools to collect, transport, process, protect and disseminate information. This affords the information advantage by facilitating net-enabled delivery of, and access to, the right information, at the right time, and in the right format. The network operations and network defense capabilities provided by Signal Soldiers are critical in enabling combat success and prevailing in the information environment.

ATP 3-36 provides the techniques for the application of electronic warfare in unified land operations. It expands on the role of electronic warfare in cyber electromagnetic activities found in FM 3-38. ATP 3-36 is divided into five chapters detailing an overview of the field, electronic warfare planning considerations, electronic warfare targeting, plan execution, and a discussion of electronic warfare in joint and multinational operations. Three appendices provide form and message formats, the basic math behind jamming calculations, and a survey of electronic warfare equipment. ATP 3-36 in final approved draft with expected publication in Summer 2014.

FM 3-38 is a new publication that codified the concept of CEMA within Army doctrine to synchronize and integrate the activities of cyberspace operations, electronic warfare, and spectrum management operations. CEMA are designed to prepare the Army to address the increasing importance that both the cyberspace domain and the electromagnetic spectrum play in the success of unified land operations. CEMA are activities leveraged to seize, retain, and exploit an advantage over adversaries and enemies in both cyberspace and the electromagnetic spectrum, while simultaneously denying and degrading adversary and enemy



use of the same and protecting the mission command system.

To fully empower commanders with the tools required to execute decisive action, the Army is aggressively pursuing ways to bring more cyberspace operations, electronic warfare, and spectrum management operations capabilities down to the tactical edge. This also includes seeking ways to provide commanders (brigade combat team and above) with an organic means to integrate

these activities into the operations process.

CEMA is integrated within the operations process via the cyber electromagnetic activities element, responsible for integrating cyberspace operations, electronic warfare and spectrum management operations into all phases of the operation. The CEMA element replaces the current electronic warfare element, but retains its staff without additional personnel. Should a specialized cyberspace operation mission

be required, the CEMA element coordinates with specialized personnel such as a cyber support element or special technical operations team that may integrate with the brigade combat team staff.

Determining how to address the challenges and opportunities that cyberspace and the electromagnetic spectrum present our forces will remain an evolving process. Time, technology, available resources, and a multitude of other factors will influence how the Army develops its solutions and doctrine. The ability to gain and maintain an advantage in cyberspace and the electromagnetic spectrum will always be vital to successful unified land operations.

This article was written with contributions from Gregg Buehler (Electronic Warfare Doctrine) and Lucas Kagel (Cyber Doctrine).

LTC Edie M. Fairbank is the U. S. Army Cyber Doctrine Branch chief.

ACRONYM QuickScan

ADRP - Army Doctrine Reference Publication
ATP - Army Techniques Publication
CEMA - Cyber Electromagnetic Activities
CoE - Center of Excellence
COMSEC - Communications Security
DODIN - Department of Defense information networks
DSCA - Defense Support of Civil Authorities
EMSO - Electromagnetic Spectrum Operations
EW - Electronic Warfare
FM - Field Manual
IA/CND - Information Assurance/Computer

Network Defense
IDM/CS - Information Dissemination Management/Content Staging
LWN - LandWarNet
NetOps - Network Operations
NM/ESM - Network Management/Enterprise System Management
SMO - Spectrum Management Operations
ULO - Unified Land Operations
VI - Visual Information
WIN-T - Warfighter Information Network-Tactical

Cyberspace training permeates professional military education

By MAJ Robert L. Collins III

As the Signal Center of Excellence transitions to the Cyber Center of Excellence, part of its mission is still to educate and develop versatile Cyber professionals to enable the Army of the 21st Century.

To some, cyberspace operations is a totally new concept emerging on a frontier where we are challenged to defend our national interests.

To others, cyberspace operations is considered a rebranding of a particular set of skills that Soldiers of the Signal Corps and Military Intelligence community share in support of a common mission.

Each of these hypotheses has merit.

The SigCoE transition to the Cyber CoE is an evolution in the way we train our next generation of digital natives and cyber warriors to fight in a domain that has no boundaries.

Today, a critical hurdle to negotiate is How do we train and educate the “old school” leaders of these new digital native, cyber warriors? It is the Cyber CoE mission to reach out beyond the gates of Fort Gordon and to integrate with the other institutions to explore every avenue of Professional Military Education and integrate cyberspace operations into the common core curriculum so that all Army leaders have the exposure to this new domain. Everyone must understand that we are engaged in a new way of fighting with impacts affecting all organizations.

All Army leaders and Department of Defense workers must transform to understand the new operational domain of cyberspace.

What must every Soldier, Army civilian, leader and commander know about the cyberspace domain and how to understand cyberspace operations as a holistic part of Joint and Unified Land Operations?

In July 2013, researchers released findings from a comprehensive study called the Army Cyberspace Leaders Development, Education, and Training Assessment and Implementation Strategy. This document addressed some important questions about the Army’s workforce.

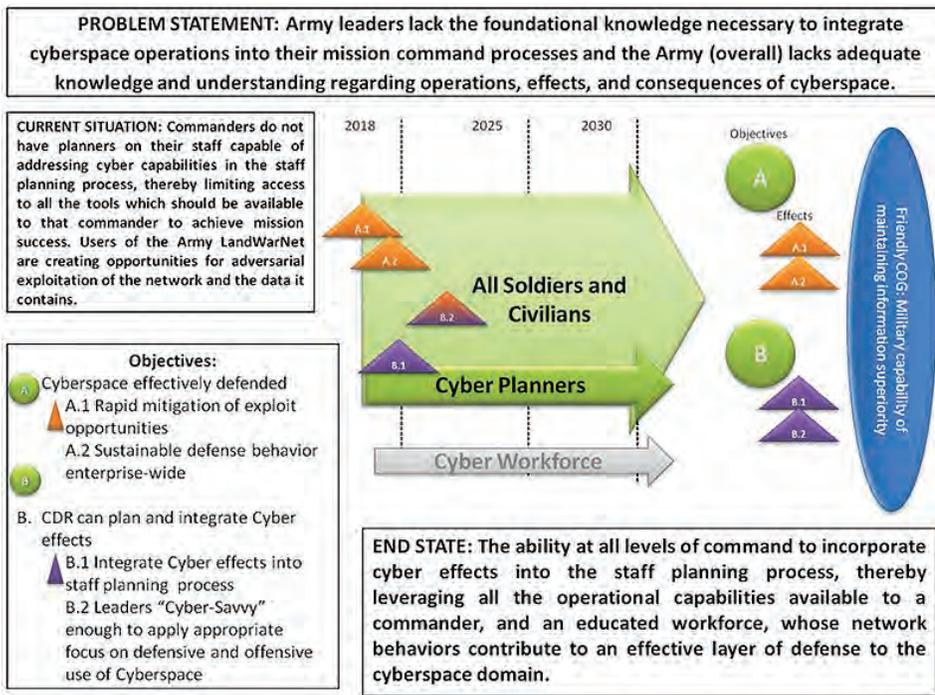
The majority of DoD personnel rely on networked systems and communications to accomplish their missions, but do not specifically conduct tactical cyberspace operations.

For purposes of the assessment and strategy, Army personnel were categorized into the following subsets: all Soldiers and civilians, leaders, staff planners and commanders. Through training and education, Soldiers, Army civilians and units achieve the technical competence that builds confidence and agility. These characteristics allow Army forces to conduct successful operations across the spectrum of conflict.

As the CCoE assumes the LDE&T mission to infuse cyberspace operations as a holistic part of Unified Land Operations, the key objective is to integrate Cyber LDE&T into Army PME to increase Army-wide knowledge of cyberspace and commanders’ ability to integrate into the unit’s operations. The strategy’s efforts will be considered successful when the following criteria are met:

- All Soldiers and civilians understand the cyberspace threat and employ or practice

Everyone must understand that we are engaged in a new way of fighting with impacts affecting all organizations.



personal behaviors and actions that contribute to defense. They must have the ability to identify a possible adversarial attack, perform initial actions, and report the incident.

- Army leaders at all levels understand effects and consequences of use, for offensive and defensive cyberspace operations in order to effectively lead, mentor, and develop their Soldiers and civilians.

Beginning with the Warrior Leaders Course for NCOs, and with pre-commissioning for officers, digital literacy and the efficient use of software and applications, as well as increasing the defensive mind-set of their Soldiers, should be a continuing topic of reinforcement.

- Army staffs fully understand and have the ability to plan for the full spectrum use of all cyberspace

capabilities within the Military Decision Making Process. Officers going in to field grade staff and command roles receive advanced operational planning and integration during Military Education Levels 3 and 4. Intermediate Level Education School for Advanced Military Studies and other Services and joint schools and academies, must provide relevant cyberspace operational knowledge that allows for the inclusion of cyberspace into the operational planning process.

- Commanders need to have a baseline understanding of their unit's cyber-related vulnerabilities and are able to integrate cyberspace operations, electromagnetic spectrum Operations, and Electronic Warfare to achieve effective cyber-related effects on the enemy.

The Cyber CoE will

continue to drive the strategy implementation by integrating cyber LDE&T into Army PME to increase Army-wide knowledge of cyberspace and commander's ability to integrate into the unit's operations. Below are current initiatives that have started and will continue under the purview of the Cyber CoE Directorate of Training:

a. The Signal Captains Career Course developers are piloting a new 40 hour module which focuses on cyberspace operations and planning. This module will be used as a baseline to develop

a new module for Captains Career Course Common Core Curriculum developed by the Combined Arms Center School of Advanced Leadership and Tactics,

b. Command and General Staff College planners have developed a one-hour block in the common core phase and a 24 hour unclassified elective at the resident Intermediate Level Education at Fort Leavenworth. Efforts are underway to develop a 24-hour classified elective for implementation in the Fall 2014. A new two-hour common core class is currently under development to replace the one-hour class.

c. The Cyber CoE will continue to partner with ARCYBER G5-7, 1st IO Command, and the School of Advance Military Studies to determine education solutions

(Continued on page 16)

(Continued from page 15)

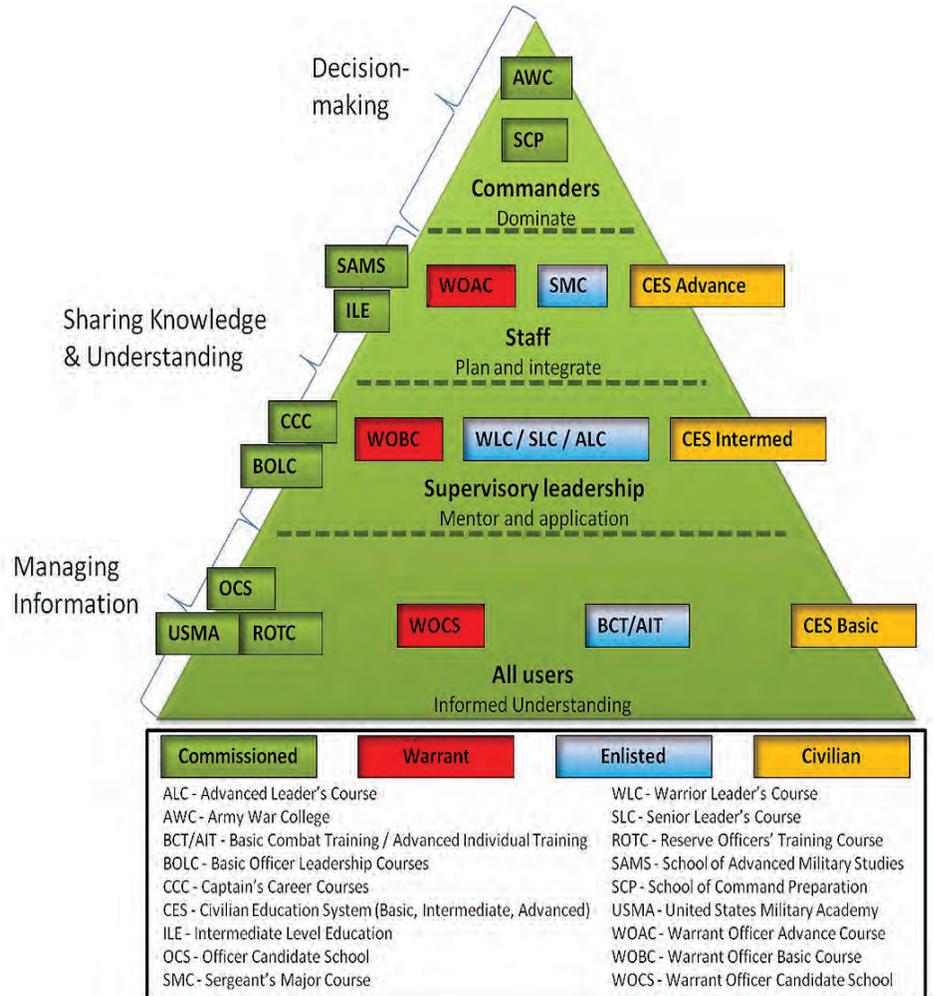
for planners being assigned to combatant commands and to educate all SAMS students on cyberspace awareness.

d. Initial development with curriculum planners to include of cyberspace operations topics in The Army War College and the School of Command Preparation.

We are members of an Army filled with professionals who take great pride in the cognitive abilities of all Soldiers – the unique ability of every member of the organization to apply critical thinking skills in every circumstance. Leveraging the capabilities, offensively and defensively in the cyberspace domain is no different from what we currently do.

We must create a knowledgeable culture where 100% of the Army, Soldiers and civilians, have a vested interest in defending our networked systems.

Leaders must mentor and develop junior personnel to be more capable of operating in the cyberspace domain. Commanders and staffs must appreciate the capabilities and effects which are available in



the cyberspace domain, both offensively and defensively, and where our operations are fully enabled, thereby enabling our domination of the information environment.

MAJ Robert L. Collins III, is currently the Deputy Director of Training at the Cyber Center

of Excellence, Fort Gordon, Ga. Prior to that, he was assigned as the Professional Leadership Division chief overseeing the management and training development for all 25A Signal Officer Training. He holds a B.S. in Mathematics and an M.S. in Information Technology Project Management.

ACRONYM QuickScan

ARCYBER - Army Cyber Command
ALM - Adult Learning Model
AWC - Army War College
CGSC - Command and General Staff College
Cyber CoE - Cyber Center of Excellence

DoD - Department of Defense
ILE - Intermediate Level Education
SAMS - School of Advance Military Studies
SALT - School of Advance Leadership and Tactics
SCCC - Signal Captains Career Course
SigCoE - Signal Center of Excellence

Wherefore came this cyber thing?

By CW5 Curtis McDonald

Have you ever asked yourself where did that word “cyber” come from?

It seems to have come out of nowhere within the last five or six years but is one of the hottest terms being used within the Department of Defense.

Looking up the word “cyber” in a dictionary generally returns definitions that list it as a connecting form or a prefix, not an actual word, itself. Some of the combinations are: cyberpunk, cyber talk, cyborg (cyber organism), cyber bullying, cyber attack, and cyberspace. Merriam-Webster defines “cyber” as: “of, relating to, or involving computers or computer networks” with its first known use being in 1991.

But the deeper truth is that today’s common usage is a shortened form of the word “cybernetics.”

Cybernetics comes from the Greek word *kybernētēs** and was combined with the English suffix *-ics*. *Kybernētēs* means helmsman/steersman or governor, from the Greek word *kybernân* which means to steer (a ship) or govern. The ending *-ics* was added because it denotes a body of facts or knowledge and often names fields of study (such as physics, ethics, politics, tactics). It is, therefore, the study of governance.

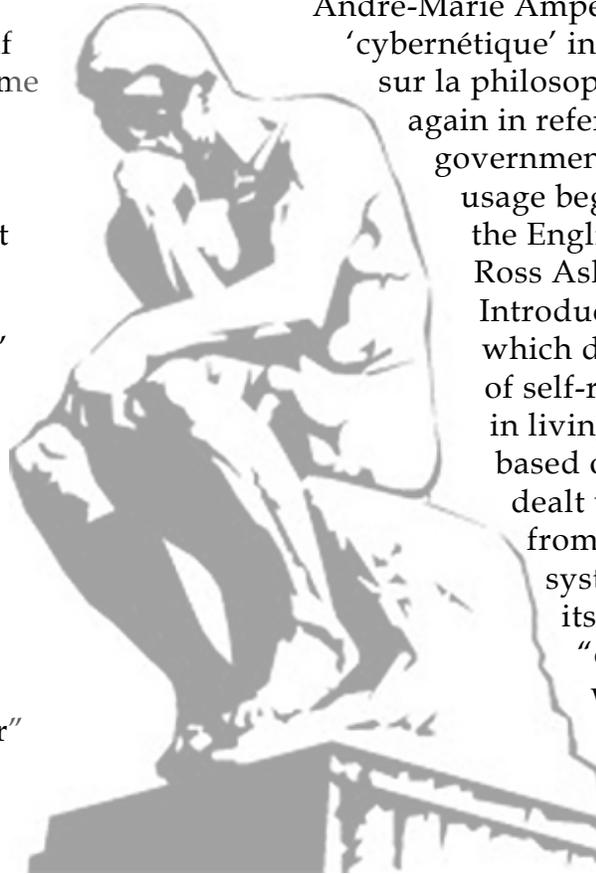
Plato used the Greek term in his “First Alcibiades”, referring to the study of self-governance of people (not machines or

biological systems). The French physicist André-Marie Ampère used the term ‘cybernétique’ in his 1834 essay “Essai sur la philosophie des sciences”, again in reference to the sciences of government. The more modern usage began with the usage by the English psychiatrist Dr. W. Ross Ashby in his book “An Introduction to Cybernetics” which dealt with the study of self-regulating systems in living organisms. It was based on a closed system and dealt with how feedback from actions within the system affected the system itself. But the term “cybernetics” gained wide acceptance when Dr. Norbert Wiener, an MIT mathematics professor who earned a bachelor degree at age 14

and a doctorate from Harvard at age 18, published his book “Cybernetics: Or the Control and Communication in the Animal and the Machine” in 1948. His book dealt with feedback and laid the theoretical foundation for advances in many technologies such as servomechanisms, automatic navigation, analog computing, and reliable communications.

The American Society for Cybernetics defines cybernetics as, “the study of systems and processes that interact with themselves and produce themselves from themselves.” While the term “cybernetics” is primarily

(Continued on page 18)



(Continued from page 17)

used within scientific academia, it has been shortened and added to other words yielding such terms as cyberpunk, cyborg**, and cyberspace.

It was science fiction writer William Gibson's short story *Burning Chrome* (1982) and novel *Neuromancer* (1984) that popularized the term cyberspace. The story lines of each dealt with computer network hacking. In *Neuromancer*, Gibson described cyberspace as, "A consensual hallucination experienced daily by billions of legitimate operators, in every nation, by children being taught mathematical concepts... A graphic representation of data abstracted from the banks of every computer in the human system. Unthinkable complexity. Lines of light ranged in the nonspace of the mind, clusters and constellations of data. Like city lights, receding."

Neuromancer also contained the first usage of the term "matrix" in reference to a visualized internet and there are parallels between *Neuromancer* and the 1999 movie "Matrix".

The term cyberspace continued to be used primarily within science fiction and virtual reality circles where it was used to loosely refer to computers or computer networks until it began to move into usage within military usage, still referring to computer networks. From Plato's usage about self-governance of people, to Ashby's and Weiner's research on feedback and systems, to Gibson's "consensual hallucination...by billions", to the American Society for Cybernetics' definition of cybernetics the common theme has been inter-

It was science fiction writer William Gibson's short story *Burning Chrome* (1982) and novel *Neuromancer* (1984) that popularized the term cyberspace described as, "A consensual hallucination experienced daily by billions of legitimate operators, in every nation... a graphic representation of data abstracted from the banks of every computer in the human system. Lines of light ranged in the nonspace of the mind, clusters and constellations of data. Like city lights, receding..."

connectedness and interaction among people and systems. That interconnectedness can be used for good or for evil, for humanity or for selfishness --indeed, for offense and defense. And that is where we find ourselves, today.

CW5 Curtis McDonald is the senior technical advisor to the Capabilities Development and Integration Directorate at the Cyber Center of Excellence. He has served 27 years as an Information Systems Technician in the Signal Corps in CONUS and OCONUS assignments and deployments.

* For pronunciation purists, let your friends and associates know that the correct pronunciation from the original Greek language is to use a "k" sound, not the "s" sound for the letter "c". Therefore the proper pronunciation is: "\ki-bor\.

**Probably the most famous cyborg was Steve Austin (Lee Majors) of "The Six Million Dollar Man" (1974-1978). Adjusted for inflation to 2014 dollars, he becomes "The 29 Million Dollar Man."

Cyberspace operations significantly impact landpower

By MAJ Irvin Oliver

As the world's populations continue increasing reliance on computer systems and networks, cyberspace will only grow in importance.

U.S. Army leaders recognize this fact and perceive a clear link between cyberspace operations and our concept of strategic landpower.

The human interaction inherent in land operations, and cyberspace is what makes strategic landpower unique. From a military perspective, leaders will utilize cyberspace to direct physical interaction, possibly against the United States, and strategic landpower encompasses all of these interactions.

As the cyber domain becomes increasingly contested, Army professionals must be prepared to successfully conduct both offensive and defensive operations that complement land operations. Although the shape of future conflicts cannot be predicted, the rapid, widespread growth in the cyber domain strongly suggests that future

“The intersection of land domain, the human domain, and the cyber domain in the future is really important for us to be successful in the future security environment.”

– GEN Raymond Odierno
U.S. Army Chief of Staff

contingency operations will require the Army to conduct effective, unified operations in cyberspace.

The Army is preparing for a future environment where the boundary between the land and cyber domain is irreversibly blurry. Our adversaries have and will continue to enhance their use of information technology to support offensive military operations, deny information and communications, and shape the battlefield. Russia's often cited cyber attacks against Georgia in support of physical attacks during their short war in 2008 preview a future role of cyber operations. Army Cyber will enable and protect Joint and Army operations, primarily in the Intelligence, Mission Command, and Protection warfighting functions in support of Strategic Landpower.

Preparation for the Future

Cyberspace will continue to grow in size and scope beyond its current position. To reflect this growing importance, the Army's Signal Center of Excellence is evolving to become the Cyber Center of Excellence, which will subsume the Signal Center and school. The Army is also continuing its establishment of the Cyber career field. The CCOE will bring signal, intelligence, and electronic warfare functions under one roof. The delineations between these three fields have become less clear as technology and the capabilities of intelligence and signal platforms grow evermore interconnected. As these systems continue to utilize and exploit the

(Continued on page 20)

same networks, seamless integration within the Army will be a necessity. The CCoE is the clearest example of this integration that will be de rigueur in the future.

The Cyber career field will provide the Army with dedicated Soldiers focused on the Cyber mission. The Army's initial investment for the Cyber career field has come primarily from the Signal and Intelligence branches of the Army. Eventually, though, the Cyber branch will develop Soldiers and leaders organically who have always been in an Army that conducts cyber operations in the same vein as combined-arms, fire support, or sustainment operations – operations that support military objectives in pursuit of strategic objectives. General Keith Alexander, the current commander of Cyber Command, is a major proponent of merging communications, intelligence, and information fields because of the common cyberspace technological foundation. This underscores the utility of cyber across the warfighting functions.

Consider a BCT deployed in support of a contingency operation. In the future, the BCT will use cyber operations to find information and develop intelligence to enable tactical operations; brigade-level communications architecture will have a cyber network as its backbone; and the defense of the BCT's networked communications, intelligence, and electronic warfare systems will be one of the ongoing missions. Cyber capabilities will also help the BCT to interact with the local population through information support operations.

Intelligence

Dedicated cyber operations at the tactical level will further enable the Army to collect and analyze information, and speed intelligence to the warfighter, which will give Soldiers the ability to act more quickly than

adversaries can prepare. They will also enable Army formations to see themselves more clearly to establish a true, real-time, common operating picture of both the physical and cyber environment. Focused cyber operations will enable staffs to improve the intelligence preparation of the battlefield by integrating ISR systems with signal and EW systems. This will promote better situational understanding, information collection, and targeting by streamlining processes and flattening system hierarchies. Tactical units will be able to directly leverage national assets more quickly and have a better defensive posture with regards to cyber operations.

The cyber domain is turning into a crucial repository for information – both friendly and enemy, and effective operations require intelligence collection and successful exploitation of this domain. Intelligence operations will always be multi-disciplinary, but the cyber element of these operations will be pervasive. The collection of information, production of intelligence, and timely dissemination will all make use of the cyber domain at the tactical and operational Army levels.

While the intelligence warfighting function centers on understanding the enemy, the physical environment, and civil considerations, cyber operations will also help the commander to make sound decisions. Awareness of the operational environment is incomplete without a clear-eyed self-assessment; cyber operations will also facilitate this improved understanding. Army network systems will carry essential elements of information that will require security and transmission in the cyber domain. This will enable commanders to make informed decisions at a speed that seizes or maintains the initiative.

Mission Command

The best intelligence and operating picture goes for naught if commanders cannot translate it into action. Mission Command

requires effective network operations and secure information systems to help commands and staffs create shared understanding through communication and information sharing. Cyber operations are essential to the mission command system by helping to organize the growing volumes of information available to Soldiers at all levels and by sharing information and ideas to ensure unity of effort.

Mission command covers more than command and control, but the timely decision making within the art of command and the systems that enable the science of control rely on clear, secure communication. Communication is the heart of mission command. Without it, achieving shared understanding vertically and horizontally is impossible. The Army's communication architecture, like any battlefield system, is vulnerable to attack. Attacks against these systems may inhibit initiative and lower prudent risk tolerance. Cyber operations facilitate mission command by maintaining networks and defending against attacks.

Adversaries will use commercial technologies and develop organic cyber capabilities to mitigate U.S. technological and doctrinal advantages. Historically, forces attack C2 systems to disrupt enemy operations, and

the future will be no different. In fact, the proliferation of technology will provide more opportunities for such attacks. The training and preparation of every Soldier encourages initiative and action within the commander's intent. As the battlefield grows to include more digital systems, however, successful attacks on Army systems may prevent exploitation of opportunities that arise from decentralized action and measured risk-taking. This makes the protection of networks and digital architecture an essential requirement for the Army.

Protection

Preserving the effectiveness of personnel, equipment, information, and networks is the heart of the Protection warfighting function. Effective protection requires forces to identify threats during the planning and execution of operations and the implementation of measures to defeat those threats. As the cyberspace operations increase, these threats will as well. As part of the Army's theater establishment functions, the protection of theater communication and intelligence networks will be a key element of Army cyber forces.

Protection of these networks and information technology systems is the clearest imperative of

Army cyber operations. As the Army increases its leverage of technology, its systems of digital networks and computer systems will be vulnerable to attack. Cyber operations to defend networks and systems will be a requirement for successful land operations across a theater of operations. Unique to the cyber domain, threats to Army and Joint networks may come from anywhere in the world. Protection against these threats will require a force that is integrated with other systems and efforts, and cyber defense must be comprehensive. It has to be part of planning at all levels and actively utilized before threats become obvious.

Cyber operations are not only a consideration for dedicated Army Cyber units. All echelons of command will need to be involved to strengthen the overall network and protection system. This starts with the continued security of non-secure internet and secure internet systems. Cyber operations must be a consideration for all commands and staffs. Additionally, given the importance of digital architecture, cyber operations and protection will be another way commanders and their staffs can weight main efforts to prevent exposure of critical vulnerabilities. Activities within the cyber domain to

(Continued on page22)

(Continued from page 21)

protect Army and Joint systems will occur throughout the operational timeline and in every phase of operations.

Conclusion

Army operations on land and in cyberspace will continue to merge and be mutually supportive.

The Army today is laying the foundation for the future force that is equally adept at operations in both domains. In the same way interaction across domains led to the development of modern air-ground integration, the integration of cyber operations will change the way the Army and the Joint force conduct operations.

Mission command, intelligence, and protection will all rely on effective and secure cyber operations to enable successful movement and maneuver, fires, sustainment, and engagement in support of the Joint force. Land operations will increasingly occur within populated areas and rely on cyberspace, and future adversaries will not only seek to disrupt and defeat U.S. operations, they will use the cyber domain to do so.

The creation of the Cyber Center of Excellence and a dedicated career field will provide the Army with a center that integrates the communication, intelligence, and electronic warfare requirements of the future. Soldiers in the Cyber field will be essential team members of commands at all echelons.

They will enable effective mission command, provide timely intelligence, and protect complex network architectures in support of Strategic Landpower and national security objectives.

In addition to a consolidated Cyber Center, the Cyber career field is an ideal location for multi-component Army units. The integration of the Total Army has been clear over the last 13 years of war, and in the future such integration will be even more important. Because of the nature of threats in cyberspace and the effects they may have at home and abroad, the Army must take an integrated approach to the cyber domain. It may be the only way to effectively provide mission command, intelligence, and protection in support of the Joint force.

Cyber operations will be a critical enabler of Strategic Landpower in a future that moves at the speed of 1s and 0s, and the current steps the Army is taking to establish the Cyber

Center of Excellence and the Cyber career field is just the beginning of an exciting chapter in the Army's history.

MAJ Irvin Oliver is a strategist (FA59) in the Commander's Planning Group at TRADOC. Prior to his current assignment, he served in the 2nd Infantry Division in the Republic of Korea and taught at the U. S. Military Academy at West Point. MAJ Oliver earned a Master of International Affairs degree from Columbia University.

[Join the Discussion](https://SIGKN.army.mil)

<https://SIGKN.army.mil>



ACRONYM QuickScan

C2 - Command and Control

CCoE - Cyber Center of Excellence

INVESTING TO SECURE THE FUTURE

*By Mr. Steve Townsend, and
Dr. Stephen B. Chaney*

This article offers a prospectus of what the U.S. Army Cyber and Signal Force must accomplish from a proponent perspective as expressed in the Force 2025 & Beyond concept framework.

You should gain an understanding of what Force 2025 & Beyond is and why it is important. The implications of the concept to the LandCyber Force are explored, and strategies of science and technology investments that position the Army for overmatch are considered.

These are exciting times in our force and ideas to succeed are presented. Some of the ideas will be quickly recognized as old and have subtle nuances that make them radically different. Other concepts in the Force 2025 & Beyond concept require a complete shift in how we think and operate as an Army.

The changes we Army professionals face in the future are vast and challenging. Transitions from execution to preparation are underway, available funding is currently diminishing, and emerging technologies offer both advantages and

vulnerabilities. Although the future strategic environment is impossible to predict with perfect accuracy, if trends continue on their present course, the U.S. Army will begin to lose overmatch by 2025.

Army professionals must adapt, evolve and innovate to meet the goals of strategic landpower. Simply put, Army leaders must plan to succeed in all military operations. Subsequently, the LandCyber Force composed of Army Cyberspace Operations (OCO, DCO, DoDIN/LandWarNet), Electronic Warfare (EA, EP, EWS), and Spectrum Management Operations, must provide leadership and capabilities to enable the Army Force for 2025 & Beyond.

What is Force 2025 & Beyond?

Continuing in fiscal year 2014 and through 2015, Army leaders will develop and refine what the Army will become. The emerging concept is titled Force 2025 and Beyond and is shaping our Army leaders' thinking about meeting the demands of the future environment in alignment with strategic priorities. The vision describes a force that is leaner, retains capability, prevents overmatch through 2025 and sets conditions for fundamental long-term change well beyond 2025. The emerging concepts for Force 2025 & Beyond in this article are attributed

(Continued on page 24)

FORCE 2025 & BEYOND TENETS

Make Army formations more expeditionary--a leaner force

Retain or improve current levels of tactical mobility, lethality and protection

Reduce required sustainment footprint in austere environments

(Continued from page 23)

to U.S. Army Training and Doctrine Command concept developers.

Force 2025 & Beyond is a comprehensive institutional campaign framework (vision, authorities, process and structure) underpinned by ideas from a hierarchy of conceptual work that Army professionals do both internally and as part of the joint force. This includes the Army Campaign Plan, the Army Operational Concept, the Strategic Landpower Concept, the Army Functional Concepts, and numerous other joint efforts. The campaign framework is organized along three lines of effort: force employment; science and technology and human performance optimization; and force design. To the broader Army audience, the Force 2025 campaign framework will operationalize how the Army will retain overmatch, and redesign the force to meet America's future needs.

Why Force 2025 & Beyond?

The Army's concept for Force 2025 & Beyond is critical for operationalizing the multi-service Strategic Landpower Concept. TRADOC language describes Strategic Landpower as the root of what is driving the changes in Force 2025 &

Beyond. Strategic Landpower is the application of landpower towards achieving strategic outcomes across the range of military operations and it recognizes the increasing confluence of land, cyber and human actions. It acknowledges that the Army is the Nation's principal land force, the Marine Corps is

an expeditionary force in readiness within the Nation's maritime force, and Special Operations Command possesses a core competency for effectiveness within the "human domain." The "Joint-ness" of operations has become an undeniable requirement for the Army to succeed.

FORCE DESIGN GOALS FOR FORCE 2025 & BEYOND

A more expeditionary Army that is mission tailored, regionally aligned and globally responsive

Leaner combat units with the same or better tactical mobility, protection and lethality

Ability to sustain itself with fewer external enablers, less dependent on a big support tail

Improved ability to counter anti-access and area denial and capable of joint entry operations

Serves as a waypoint for the Force of 2040; not an end in itself

Although the Army, Marine Corps, U.S. Special Operations Command, and USCYBER Command are designed for different purposes, their purposes intersect in the land domain. Thus, the reality is that the operational environment is going to necessitate some changes in the Army's ideas of strategic landpower, such as maneuvering strategically, expeditionary maneuver, and addressing the human nature of war while interweaving and understanding cyberspace operations.

The U.S. Army in 2025 will be regionally aligned and forward engaged. It must be able to deter conflict and build partner networks, gain understanding, and achieve positional advantage that sets conditions, prevents conflict, and shapes the operational environment while having its eyes open to its own capabilities, as well as others.

Required Capability: Force 2025 and Beyond will operationalize Army support to the Strategic Landpower concept of maneuvering strategically – the employment of landpower short of war

This Force in 2025 is extremely expeditionary, mission tailored, and globally responsive. It must be informed, capable and able to use discriminate power in close operations among the people, while leveraging an agile mix of both lethal and non-lethal action to control events. Expeditionary maneuver will drive fundamental change in the design of the force. We must position today for this change.

Required Capability: Force 2025 & Beyond will operationalize Army support to the Strategic Landpower concept of expeditionary maneuver - landpower at war.

Understanding the human nature of war is critical to the Army of 2025. We must understand how tactical actions interact with populations. We must understand their larger impact on achieving strategic ends. The Force in 2025 must be adept at influencing populations, governments, and other militaries, and prepared to execute

across the range of the human enterprise and social dimensions as a core role for conventional forces. This concept requires Special Operations and Conventional Forces to work together in unprecedented ways. A caution about combat overmatch: those efforts not focused on a human objective often have failed historically to secure strategic success. Thus, the Force in 2025 and beyond must effectively leverage the increasing convergence of the land and cyber domains and the "human domain." Clearly, the level of intensity, the pace, and tempo of human interaction is tremendously accelerated by cyberspace and the human interaction in that domain and the land domains.

Required Capability: Force 2025 & Beyond will operationalize Army support to the central and essential role of Strategic Landpower - understanding, influencing, or exercising control within the "human domain."

LandCyber Force - enabling the Army Force for 2025 & Beyond

The LandCyber White Paper prepared by ARCYBER in coordination with ARCIC and the Cyber Center of Excellence describes a transformational concept: Land and Cyber are merging domains. The paper further offers relevant information to all Army organizations that develop or use Army cyberspace doctrine, organization, training, materiel, leadership and education, personnel, and facilities requirements and capabilities. In other words, if you operate in cyberspace, you should take a look at how we are moving forward and what is expected in the coming years of change. The cyberspace domain grows more contested, congested, and competitive. Land Forces rely more heavily than ever on cyberspace to shoot, move, communicate, and make command decisions. What happens when an adversary, an unassuming bystander, or a friendly operator in cyberspace denies our Army

(Continued on page 26)

(Continued from page 25)

freedom of maneuver. How can we support, protect, and attack in cyberspace to ensure successful Unified Land Operations? This interdependence is the driving force behind LandCyber. It is a fresh perspective on old problems and new threats that we face today, in 2025 and beyond. It is the reason the Army must invest to secure the future.

Today's Investments to Secure the Future

One of the design goals for Force 2025 & Beyond is acknowledgement that Force in 2025 is a way point to the Force beyond 2025. It is not an end in itself. Clearly, we have to think through deeper than 2025, because most of what we come up with in terms of capability will be a way point or an interim solution to meet the needs of the Army beyond 2025. The three lines of effort that comprise the Force 2025 and Beyond campaign framework help to describe how the Army will invest resources of today to secure the deep future.

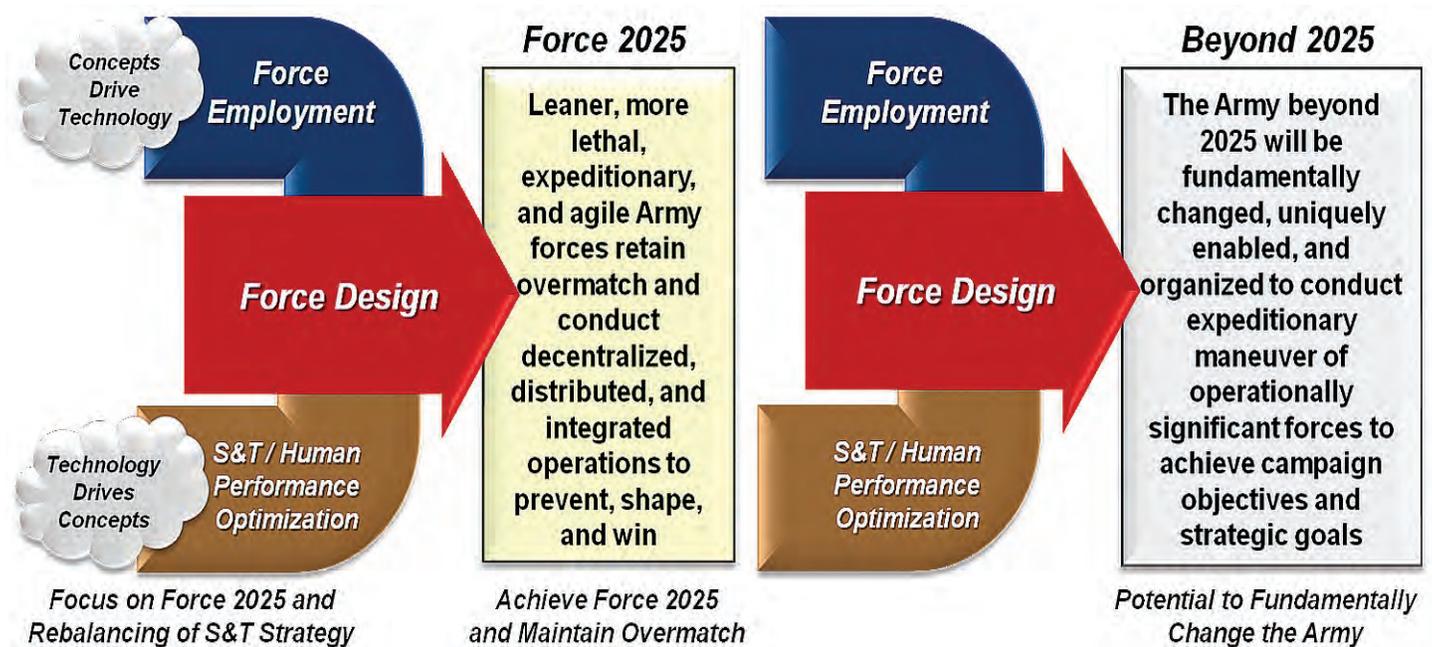
The Force Employment line of effort focuses on changes to force employment that enables the Army to operate differently. The principle effort focuses on the conceptual work that the Army does to produce documents

that describe the ideas which underpin how Force 2025 operates. Today, Army concepts and doctrine focus the Army on combined arms maneuver, wide area security and special operations. The complex operational environment of Force 2025 & beyond however requires the Army to operate differently.

The future Army operates decentralized, distributed, and integrated among combined arms capabilities, special operations forces, and with unified action partners.

The Science and Technology and Human Performance Optimization line of effort focuses on enabling the force differently with balanced technology investments that deliver incremental improvements and S&T efforts with leap-ahead potential. The principle effort focuses on development of a coordinated modernization plan to achieve a more expeditionary BCT while retaining capability, preventing the loss of overmatch through 2025, and setting the conditions for fundamental change beyond 2025. The implications of S&T on Force 2025 and Beyond requires deliberate coordination among all Centers of Excellence to reprioritize science and technology needs with a goal to enable the force through prioritized needs that are as effective and efficient as possible.

The Force Design line of effort represents



the convergence and reconciliation of the first two lines of effort to organize differently. In this line of effort, the Army develops an operational and organizational concept for the Army to meet the requirements of 2025. Force design combines the changes to force employment with the enhancements of S&T and human performance initiatives to inform the design of new or modified Army organizations. The principle effort focuses on validating the ideas across the lines of efforts using experiments, evaluations, exercises, wargaming, and other efforts to determine just how the Army organizes and designs the force. Ultimately, in the operational and organization concept for Force 2025, the Army outlines organizational structures and integrated DOTMLPF solutions needed to optimize the force to accomplish its assigned missions in the future.

Cyber Center of Excellence: S&T

The implications of Force 2025 and Beyond on S&T presents a tremendous opportunity for COEs to partner in new ways with the S&T community. That is exactly what the Cyber COE is doing with the U.S. Army Materiel Command/ Research, Development and Engineering Command, the Communications-Electronics Research, Development and

THE VALUE OF CANDIDATE TECHNOLOGIES IS BASED ON THE FOLLOWING QUESTIONS:

Does the technology enable the United States to maintain overmatch?

Does the technology maintain or increase the capability of units and enable more expeditionary brigade combat teams?

Does the technology enable combat units to be more self-sustaining or conversely reduce the logistical demand?

Engineering Center, and even the Defense Advanced Research Projects Agency. This partnership continues to develop and involves defining the future force objectives for the tactical network, Cyber, and Electronic Warfare required capabilities, and shaping the research and development activities with the S&T community along the way.

The Cyber COE's approach to optimize the future force takes two directions. One is where concepts drive the technological research and development that can translate into capabilities

within the acquisition process to mitigate capability gaps. The other approach is analysis of promising technology already under development within the S&T community that can be aligned to Force 2025 & Beyond.

The Cyber COE S&T priorities principally center on capability and modernization across our proponenty areas. However, our S&T priorities also allow us to analyze the depth of our formation and the ability to make it leaner in the context of the amount of effort we

(Continued on page 28)

(Continued from page 27)

allocate towards the force of 2025. We see the potential to lower procurement costs and decreasing the number of tasks required to configure and maintain what used to be several separate discrete systems, thus reducing operator tasks and complexity too. We also see potential to reduce the logistical tail and the number of field contractor support representatives. In some cases, such as automation of cyber functions, there is even potential to reduce the cognitive work load on the Warfighter.

Conclusion

The future threats to the Army's LandCyber Force are uncertain, daunting, and complex. Adaptive approaches, evolutionary concepts, and innovative solutions are required to maintain the overmatch

that is enjoyed today by the Army. Today's security, cyber, and maneuver capabilities rest on 1990-2000's investment strategies. These decisions were made long before Apple released the first iPhone on 29 June 2007. The next generation of Warfighters require the best available technology, an optimized force design, and an in-depth understanding of the complexities of future warfare. Investments in these areas today position the Army to maintain overmatch and fundamentally change to meet the challenges to Army Force 2025 & Beyond.

Steve Townsend is currently the Concepts Branch chief in the Concepts and Analysis Division, Capability Development Integration Directorate, U.S. Army Cyber Center of Excellence. He has a Bachelor of Science in Information Technology with a concentration

in Advanced Networking from the University of Phoenix. He has worked as a lead concepts developer for the Signal/Cyber COE and is the COE's lead for the Army's Unified Quest series of wargames and future studies, and the TRADOC Campaign of Learning.

Dr. Stephen Chaney is currently the Senior Operations Research and Systems Analysts in the Analysis Branch, Concepts and Analysis Division, Capability Development Integration Directorate, U.S. Army Cyber Center of Excellence. He has a PhD in Physics from the University of Georgia. He has worked as an analyst for the Army and Joint forces at the Army Materiel Systems Analysis Activity, the Joint Task Force Paladin-Afghanistan, the Joint Improvised Explosive Device Defeat Organization, and the Cyber CoE.

ACRONYM QuickScan

ARCYBER - U.S. Army Cyber Command
ARCIC - Army Capabilities Integration Center
CoE - Center of Excellence
DCO - Defensive Cyber Operations
DODIN - Department of Defense Information Network
DOTMLPF - Doctrine, Organization, Training, Materiel, Leadership, Personnel, and Facilities
EA - Electronic Attack
EP - Electronic Protection

EW - Electronic Warfare
EWS - Electronic Warfare Support
GPS - Global Positioning System
LOE - Line of Effort
NetOps - Network Operations
OCO - Offensive Cyber Operations
PNT - Position, Navigation, and Timing
TRADOC - U.S. Army Training and Doctrine Command
RF - Radio Frequency
SATCOM - Satellite Communications
S&T - Science and Technology



BUILDING THE CYBER-ELECTROMAGNETIC CAREER FIELD

By Office Chief of Signal Staff

This article is designed to dispel some of the assumptions circulating through the Regiment about the changes evolving in the Signal career field.

Examples of some of the rumors making the rounds include: (1) Military Occupational Specialty 25D and 255S were originally developed specifically for the Cyber-Electromagnetic workforce and thus will move to the CEM Career Field when established; (2) because there are more 255A personnel authorized in Cyber Mission Force units than any other Signal warrant officer MOS, MOS 255A will also move to the CEM CF when established; and (3) because Cyberspace Operations consists of Offensive Cyberspace Operations, Defensive Cyberspace Operations

and Department of Defense Information Network Operations, all Army Network Operations MOSs will move to the CEM CF as a component of DODIN when established.

Not only are these assumptions inaccurate, but it is way too early in the development of the future CF to leap to such conclusions.

Before diving into some details on building the CEM CF, developers in the Office Chief of Signal along with others within the community of interest must first determine what makes a CEM MOS and then distinguish it from MOS of other career fields. While most of this article cites enlisted Signal MOS, the information is illustrative of analysis being performed on warrant officer MOS, officer Functional Areas,

(Continued on page 30)

(Continued from page 29)

and branch officer Areas of Concentration and those of other branches.

Network Operations consists of three elements: content management, network management, and information assurance (now cybersecurity)/computer network defense. As we move forward, NetOps will remain a core competency of the Signal Corps.

Additionally, NetOps is now holistically associated with the Cyber CoE under its force modernization proponent functions of Signal/communications network and services, and cyberspace operations.

Doctrinally, NetOps is the Army's operational contribution to the Joint DODIN mission. As such, we then delineate the Cyberspace Operations components of OCO and DCO as two of the main functions, along with electronic warfare, that are the current focus of the CEM CF.

MOS 25D, for example, is a new MOS created by divesting emerging critical tasks to support NetOps functions and work roles from MOS 25B to this new MOS. There are two key elements driving the decision to create MOS 25D. First, we realized that the growing number of functions assigned to MOS 25B were inadvertently over-broadening the MOS. The warrant officer occupational specialty work already done delineated CND

as a separate MOS. Second, the concurrent efforts leading to the published All Army Activities (ALARACT) 228/2008 (a classified document) directed Army leaders to tailor existing capabilities and: (1) track trained personnel, (2) prevent loss of perishable skills, (3) provide an enduring cradle-to-grave career path, and (4) meet doctrinal/organizational positional requirements.

The 25D MOS was then a personnel capability created to fill well over 600 positions in Active Army organizations (560 in National Guard units and 170 in Army Reserve units) predominantly in brigades, divisions and corps to perform deliberate coordinated actions to modify information systems or network configurations in response to CND alert or threat information.

In order to perform these duties, specific accessions prerequisites emerged which include the ability to obtain a Top Secret/Sensitive Compartmented Information security clearance, a specific aptitude as measured by Army entrance testing and specifically established assessment tests, four years documented experience in information technology, Cybersecurity certifications, computing environment certifications, leadership training, and even a minimum grade requirement.

More information is available in the 25D frequently asked questions article also in this edition of the Army

Communicator on page 33.

Moving to the CEM CF, the first notable difference from the 25D example above is the emerging prerequisites derived from the tasks and functions required by the assigned cyber mission force work roles.

While the documented responsibilities for MOS 25D necessitate squad/platoon leadership abilities and the ability to operate with little to no supervision, the significant oversight and extreme rigor in execution of the cyber work roles due to the significance of even a singular keystroke in error preclude such prerequisites.

Additionally, 25D experiential and certification requirements necessary to perform deliberate coordinated actions to modify the broad scope of both information systems and network configurations is significantly different from the CyMF work roles that are much narrower and more precise in focus. Accordingly, initial prerequisites are considerably different between the two career field MOS.

Finally, career progression from an initial entry position to subsequent positions of greater responsibility differ significantly as well. MOS 25D, for example, will be required to maintain a deep understanding of a broad range of information technology devices to include servers, routers, end user terminal devices, etcetera; their mission field as localized

defenders will include everything networked in the LandWarNet environment. Conversely, initial indications are that CEM personnel will be employed into specific work roles focused on a much narrower range but progressing to much deeper levels as part of a much larger team whose mission field accumulatively is much larger. Therefore there is evidence for the need of a separate and distinct cyber career field

So, how does one create a career field in the Army?

Since a career field is a specific grouping of functionally related officer, warrant officer, enlisted, and civilian positions into management categories having a common mission area, and since an MOS identifies a group of duty positions that requires such closely related skills, the easy answer is that the career field will be created as the associated MOS, AOC, and/or FA are created. While it may be a foregone conclusion, Army leaders must first determine that a new MOS is required and then submit the action that does so. What follows are some of the major muscle movements used to determine the need to create a new MOS.

The impetus is most often the reception of an actual or perceived personnel performance deficiency. These are normally derived from lessons learned, commander's comments, tasking orders, or even directed by senior leadership. The next step includes essential research and analysis to determine the validity of the perceived performance deficiency and identify which Army echelons and elements are affected. All of this analysis must be validated because Army leaders will not support the creation of a new MOS without rigorously validated requirements.

This validation begins by conducting a needs analysis to determine the true cause of the deficiency. Needs analyses are much broader than simply focusing on the perceived personnel deficiency. Doctrine, organizational structure, training and even associated existing MOSs are included in order to both funnel

problems to the correct Doctrine-Organization-Training-Materiel-Leader Development-Personnel-Facilities solutions as well as to determine if the challenge has been introduced by emerging skill requirements. Emerging skill requirements is an indicator for the need to address other DOTMLPF functions.

If no other possible solutions exist other than the creation of a new MOS, the assigned Capabilities Development Integration Directorate analyzes the force requirements to determine the actual count and specific location by COMPO, echelon and element, paragraph, and line number of each position that is tasked to provide the functional capability required. CDID will also provide a risk assessment on the capability deficiency remaining unresolved. If the risk assessment is measured as high to medium, and cannot be solved other than through a personnel solution, the assigned Personnel Proponent Office initiates an MOS Concept Feasibility Study.

The Concept Feasibility Study is another multifaceted event that consists of the following major parts. First the determination of subject areas/functions/tasks placed under this MOS; this is also the start of a new job description. The PPO will then prepare a list of tasks (both known and projected) to be performed by the new MOS. These tasks must be charted by echelon and element and must also be characterized by notional skill levels performing the tasks (e.g., SL 1 and SL 2 or SL 3 only, etc.). The PPO then writes a macro training strategy memo that now includes the derived MOS prerequisites.

The associated Directorate of Training then convenes a subject matter expert critical task board and physical demands analysis panel. DOT also prepares appropriate course administrative data documents to support a Military Occupational Classification Structure action submission and endorses the training annex.

Based on all of the input from above, the

(Continued on page 32)

(Continued from page 31)

PPO then determines the size of MOS, works a Total Army Authorizations Documents System cross-walked spreadsheet of required and authorized positions that are part of the MOS in which to identify all positions. All of this helps the PPO to determine appropriate grade distribution and develop initial standards of grade tables.

This entire packet is then presented to the PPO director along with a feasibility study displaying the ability to provide a viable career path from entry grade (private or noncommissioned) to SGM for approval and then presentation to the commanding general/ chief of the branch.

Once the commanding general approves the packet, it is assembled for submission to U.S. Army Training and Doctrine Command for staffing

concurrency and their release to Headquarters Department of the Army.

So, where are we today with building the CEM CF?

Remember the comments on doctrine and the identification of functional capabilities required?

Army Field Manual 3-12 will become the underpinning doctrine for the future CEM CF. Work on FM 3-12 is underway but not expected to be final for another 12-18 months.

However, work building toward the career field is underway and many of the experts crafting FM 3-12 are concurrently shaping the CEM CF.

Army leaders must be cautious, however, to not allow the "P" to get too far ahead of the "D" and the "O" of the DOTMLPF process.

There is a reason the P is much further down the acronym as most of the other components inform the building

of the personnel functions. Will Army leaders look to personnel in existing MOS such as 25D and 35Q to reclassify into the new 17-Series MOS when they become available? The answer is yes, without question.

Will there be 17-Series MOS authorized outside the units currently identified within the CyMF today? The answer is most likely.

Will MOS 25D, 35Q, and 255S all be subsumed into CF 17? That is not likely at this time...but without further development of evolving doctrine to include concepts of operations, concepts of employment, field manuals, etc., we are moving cautiously and deliberately to meet the Chief of Staff of the Army's direction to have CF 17 and its associated branch stood up by 1 October 2016. Challenging? Yes.

Impossible? Never say never!

ACRONYM QuickScan

AOC - Area of Concentration
CEM - Cyber-Electromagnetic
CDID - Capabilities Development Integration Directorate
CF - Career Field
CND - Computer Network Defense
CoE - Center of Excellence
CyMF - Cyber Mission Force
DCO - Defensive Cyberspace Operations
DODIN - Department of Defense Information Network Operations
DOT - Directorate of Training
DOTMLPF - Doctrine Organization Training Materiel Leader Development Personnel Facilities

FA - Functional Area
FAQ - Frequently Asked Questions
HQDA - Headquarters Department of the Army
MOCS - Military Occupational Classification Structure
MOS - Military Occupational Specialty
NetOps - Network Operations
PCO - Offensive Cyberspace Operations
PPO - Personnel Proponent Office
SL - Skill Levels
TRADOC - U.S. Army Training and Doctrine Command
TS/SCI - Top Secret/Sensitive Compartmented Information

25D Frequently Asked Questions

Here are the answers to some questions that have been asked about the changes in Signal career fields that are evolving as cyberspace functions and responsibilities expand.

Q1: Why must applicants provide four years of documented experience in Information Technology and Cybersecurity?

There are actually three components to this answer: (1) to meet Joint Computer Network Defense-Service Provider experiential requirements outlined in DoD 8570.01M, (2) in order to successfully enter the rigorous training environment of the 25D transition course, and (3) because all 25D are expected to perform deliberate coordinated actions to modify information systems or network configurations in response to CND alert or threat information which necessitates Knowledge, Skills, and Abilities gained through experiential learning over the course of four years in IT and CS systems; we don't want our 25D to inadvertently create vulnerabilities or disrupt command and control systems due to second and third order effects of their actions.

Q2: Why must applicants be Information Assurance Technical Level II or IA Management Level I certified?

Similar to the experience level above, elevated System Administration privileges are required to perform CND-SP duties for which both Joint (i.e., DoD 8570.01M) and Army (i.e., AR 25-2) policy and regulations require specific certifications. If anything, these experience and IA certification requirements are expected to become more precise and stringent as the Joint

Information Environment becomes a reality.

Q3: Why must applicants hold the appropriate Computing Environment certifications?

Similar to above, not only does DoD 8570.01M and AR 25-2 mandate IA, IAT, and IAM requirements, CE certifications are also required to operate with elevated System Administration privileges within each specific computing environment.

Q4: Why must applicants be Advance Leaders Course graduates?

The documented responsibilities for MOS 25D necessitate squad/platoon leadership abilities and the ability to operate with little to no supervision. ALC is the Army's NCOES school that teaches squad/platoon leadership abilities and prepares enlisted Soldiers to lead and direct small teams.

Q5: Why must applicants be a staff sergeant with at least eight years Time in Service but less than 17?

As already stated above, the documented responsibilities for MOS 25D necessitate squad/platoon leadership abilities and the ability to operate with little to no supervision. Additionally, 25D personnel must perform deliberate coordinated actions to modify information systems or network configurations in response to CND alert or threat information. These characteristics (i.e., little to no supervision and the ability to

(Continued on page 34)

(Continued from page 33)

modify information systems or network configurations) and the significance to the consequences if abused or if done in error require a more mature Soldier/leader.

Finally, the three year active duty service obligation incurred is best if not infringed upon by a Soldiers' desire to retire; hence the not more than 17 years TIS.

Q6: Why is COMSEC part of the 25D MOS?

By doctrine Communications Security is a subset of Information Assurance that provides the capability to deter unauthorized access or alteration of information and related materials. It was determined during the initial development phase in 2009 to thus include this work role with the CND-SP work roles from MOS 25B to MOS 25D. As the DoD moves to Key Management Infrastructure and beyond, COMSEC will be an integral aspect of defense in depth woven into the very fabric of the network defense systems and methodologies. Having one MOS singularly responsible is extremely important.

Q7: What would happen if COMSEC were removed from MOS 25D?

In creating an MOS in

the Army, sufficient force structure is critical to ensure adequate numbers of junior grade positions exist to support the appropriate senior grade structure required. Adequate numbers of senior grade positions must exist to ensure sufficient opportunity for promotion and career progression.

Approximately one-half of the Active Army positions targeted to become 25D are associated with COMSEC. Should these position be excised from MOS 25D, the entire 25D force structure becomes extremely out of tolerance, unstable and unsupportable. Such a move would require another Military Occupational Classification Structure action and if the resultant MOS structure could not sustain an MOS, it would not be approved by HQDA G1.

Q8: If assigned as a 25D to a COMSEC custodial position, will I be stuck in the vault?

In the past, many 25Bs have been assigned to COMSEC custodial positions. Since these positions are assigned outside of the network and content management sections, these Soldiers were often not granted elevated System Administration privileges. This often prevented them from working in their other primary skill sets when not

engaged in COMSEC custodial duties.

Also, since COMSEC training was not a core component of MOS 25B training and because units usually lost Soldiers for several weeks to attend a COMSEC certification course, Soldiers trained in COMSEC often found themselves in repetitive assignments in COMSEC custodial positions quickly atrophying their IT skills.

In the future, all 25Ds will be certified to perform COMSEC custodial duties. This means that while one of the four 25D assigned to a Brigade Combat Team, for example, will be assigned as the COMSEC custodian, the remaining three can all be assigned as alternate COMSEC custodians.

The COMSEC position will also be under the supervision of the 255S assigned over the network defense section of the BCT S6. This means all 25D will be granted elevated System Administration privileges. The 255S will therefore have the ability to rotate all four 25Ds through COMSEC custodial duties ensuring all remain competent on the required KSAs to perform these duties, but more importantly, allowing all four 25Ds to remain actively engaged in performing deliberate coordinated actions to modify information systems or network configurations in response to CND alert or threat information.

The direct answer to this question is no, you will not be stuck in the vault.

Q9: Will MOS 25D become a Cyber Electromagnetic Career Field MOS?

It is possible that MOS 25D will become a cyber electromagnetic career field.

However, MOS 25D was specifically created to meet the Signal/Communications Network and Services IA/CND requirements predominantly in brigade through corps units. These requirements continue to exist today. All analysis done to date indicate that the 17-Series MOS envisioned to be a part of the CEM CF require significantly different accessions criteria. The career path for the 25D and future 17-Series MOS are significantly different and current efforts are to create MOS specific for the CEM CF. In light of these facts, most Soldiers qualified

to meet the 25D accessions prerequisites will find that they are also qualified to meet the future 17-Series accessions prerequisites. The opposite, however, may not be true.

Q10: I heard that all 25D are being assigned to the 7th Signal Command at Fort Gordon, how can I become a 25D and be assigned to a brigade or division?

Currently leaders in the U.S. Army Cyber Protection Brigade being stood up under the 7th Signal Command (Theater) at Fort Gordon Ga., have priority with first-right-of-refusal for Soldiers converting to MOS 25D. This is being done as a bridging strategy to grow combat power in Cyber Mission Force units.

Many of these positions within the CPB to be coded 25D will be reviewed for conversion to a 17-Series MOS once that career field has

been established. Similarly, many Soldiers assigned to the CPB will be assessed for reclassification to a 17-Series MOS.

Qualification for reclassification to MOS 25D does not automatically grant one an assignment to the CPB. However, the 7th SC(T) leaders have their own unit assessments and interview process to select or non-select Soldiers for assignment.

Soldiers qualified for MOS 25D who are non-select for the CPB will be trained and assigned to other priority fill 25D positions throughout the Army. Many of the priority fill positions are in brigades and divisions.

The work and development for future Career Field 17 is underway and of a high priority Army leaders.

Extraordinary measures are being reviewed that could result in radical shifts in personnel policies and management systems. Until the dust settles, be prepared for the otherwise unthinkable.

ACRONYM QuickScan

ALC - Advance Leaders Course
BCT - Brigade Combat Team
CE - Computing Environment
CEM - Cyber Electromagnetic
CF - Career Field
CND - Computer Network Defense
COMSEC - Communications Security
CPB - Cyber Protection Brigade
CS - Cybersecurity
DoD - Department of Defense
FAQ - Frequently Asked Questions

G1 - Personnel/Administration Management
HQDA - Headquarters Department of the Army
IA - Information Assurance
IAM - Information Assurance Management
IAT - Information Assurance Technical
IT - Information Technology
JIE - Joint Information Environment
KSA - Knowledge, Skills and Abilities
MOS - Military Occupational Specialty
SP - Service Provider
TIS - Time in Service

Human Resources Command stands up new Cyber Branch

By LTC Chevelle Thomas

The U.S. Army Human Resources Command established a provisional Cyber Branch in March 2014, to provide career management, development and readiness to the Army's cyber forces.

The establishment of the branch will ensure the

Army maintains visibility of Soldiers with unique cyber skills and talents, according to officials with Human Resources Command, or HRC. The new branch will perform career management services and provide Soldiers with cyber skills a "focal point" within HRC, said MG Richard P. Mustion, commanding general, HRC.

"While there are a significant number of decisions yet to be made on the future of the Army cyber force, we must establish an element dedicated to the assignment and career management of cyber Soldiers," said COL Robert E. Duke, chief of Operations Support Division, Officer Personnel Management



The new Cyber Branch will provide career management services to 29E electronic warfare specialists and officers who serve in cyber operations or cyber planning.

Directorate, HRC. "We will retain enough flexibility in our approach at HRC to adjust to changes as cyber proponency matures, and [as] this force evolves to meet mission requirements."

"As the Army develops cyber capability and establishes a Cyber Electromagnetic Branch, HRC remains aligned by providing capable and dedicated personnel support to this emerging workforce," said COL Duke. "We are establishing a Branch that consolidates enlisted, warrant officer and officer management and combines functional or designation focus with an organizational focus."

This is different from traditional branch management where one branch manages officers and an entirely different branch manages enlisted personnel. The Cyber Electromagnetic Branch, or CEM, branch will be a hybrid that consolidates and holistically manages the efforts of the entire Army cyber population under one entity, HRC officials said.

"This will enhance stabilization and the ability to gain depth into the specialized field," said LTC Candice E. Frost, Operations and Plans chief of Officer Readiness Division, OPMD, HRC. "As the Army's Cyber Center of Excellence stands up, the management of movement into and out of the cyber force rests upon Army Cyber's leadership and HRC's approval."

This closely aligned relationship will allow the Cyber or CEM Branch to better support a small, highly skilled, high-demand population in order to maintain personnel readiness in line with Army priorities, said Duke.

"The process is designed to ensure cyber force leadership has visibility of Soldiers with unique cyber skills and mechanisms in place to ensure a stable force capable of executing cyber missions," said LTC Kurt Connell, Military Intelligence Enlisted Branch chief, Enlisted Personnel Management Directorate, HRC. "What we don't want to do is create inadvertent turbulence in the cyber formation.

So, as we set the conditions for incoming and outgoing Soldiers, control mechanisms are collectively agreed upon for each personnel action or assignment to meet both the needs of the Soldier and the Army."

A key part of managing the force is identifying the distinct groups that make up the population in constructing the branch, officials said. The initial organization is established around a set population of military occupational specialties, known as MOSs, additional skill identifiers, or ASIs, and current positions held by individuals in the cyber field.

The CEM branch centers on Functional Area 29, Area of Concentration 29A, MOS 29E and 290A.

Additionally, it supports individuals in cyber operations, and those who function as cyber planners or defenders and receive an ASI or Skill Identifier of E4. Awarding this ASI is done by Army Cyber Command and is based on the individual Soldier, unit and mission, HRC officials said. It is not MOS dependent, they said.

"Development of an ASI/SI to identify those who provide support to cyber is underway," LTC Frost said.

Factors such as population management, current and future requirements, training necessities, and growth and maturity within the field may also influence cyber assignments, HRC officials said.

"The personnel requirements are greater than the number of people available to fill them," COL Duke said.

"Developing a mature force able to meet all Army requirements will take time; many assignments can require technical training and a lot of lead time. Training an individual throughout the entire process from recruiting, accessing, entry-level training and other professional military educational objectives to the point of where they can function within the career field of operations is sometimes extensive."

Army researchers looking to blend electronic warfare

By Kristen Kushiya

As new technologies emerge and new cyber and electronic warfare threats plague Soldiers in the field, U.S. Army scientists and engineers continue to define next-generation protocols and system architectures to help develop technology capabilities to combat these threats in an integrated and expedited fashion.

As part of the Integrated Cyber and Electronic Warfare, or ICE, program, the U.S. Army Research, Development and Engineering Command's Communications-Electronics Center, known as CERDEC, researches the technologies, standards and architectures to support the use of common mechanisms used for the rapid development and integration of third-party cyber and electronic warfare, or EW, capabilities.

"Currently, within cyber and EW disciplines there are different supporting force structures and users equipped with disparate tools, capabilities and frameworks," said Paul Robb Jr., chief of CERDEC Intelligence and Information Warfare Directorate's Cyber Technology Branch.

"Under the ICE program, we look to define common data contexts and software

control mechanisms to allow these existing frameworks to communicate in a manner that would support the concurrent leveraging of available tactical capabilities based on which asset on the battlefield provides the best projected military outcome at a particular point in time," said Robb.

The boundaries between traditional cyber threats, such as someone hacking a laptop through the Internet, and traditional EW threats, such as radio-controlled improvised explosive devices that use the electromagnetic spectrum, have blurred, allowing EW systems to access the data stream to combat EW threats, according to Giorgio Bertoli, senior engineer of CERDEC I2WD's Cyber/Offensive Operations Division.

Additionally, significant technological advancements including a trend towards wireless in commercial applications and military systems have occurred over the last decade, said Bertoli.

"This blending of networks and systems, known as convergence, will continue and with it come significant implications as to how the Army must fight in the cyber environment of today and tomorrow," said Bertoli.

"The concept of technology convergence originated as a means to describe the amalgamation of traditional wired versus wireless commercial services and applications, but has recently evolved to also include global technology trends and U.S. Army operational connotations -- specifically in the context of converging cyber and EW operations," said Bertoli.

The Army professionals find themselves in a unique position to help mitigate adverse outcomes due to this convergence trend.

"Post-force deployment, the Army has the vast majority of sensors and EW assets on the tactical battlefield compared to any other service or organization, posing both risks and opportunities. Our military's reliance on COTS [commercial-of-the-shelf] systems and wireless communications presents a venue for our adversaries to attack. Conversely, the proximity and high density of receivers and transmitters that we deploy can be leveraged to enable both EW and cyber operations," said Bertoli.

"The ability to leverage both cyber and EW capabilities as an integrated system, acting as a force multiplier increasing the



Photo illustration courtesy of the U.S. Army Research, Development and Engineering Command's Communications-Electronics Center

Developers in the U.S. Army Research, Development and Engineering Command's Communications-Electronics Center Integrated Cyber and Electronic Warfare, or ICE, program look to leverage both cyber and Electronic Warfare capabilities as an integrated system to increase the commander's situational awareness. CERDEC leaders are focusing their development efforts on researching solutions to address specific cyber and Electronic Warfare threats and developing the architecture onto which scientists and engineers can rapidly develop and integrate new more capable solutions.

commander's situational awareness of the cyber electromagnetic environment, will improve the commander's ability to achieve desired operational effects," said Robb.

A paradigm shift in how the Army views system and technology development will further enhance CERDEC's ability to rapidly adapt to new cyber and EW threats.

"The biggest hindrance we have right now is not a technological one, it's an operational and policy one," said Bertoli. "The Army [leadership] traditionally likes to build systems for a specific purpose - build a radio to be a radio, build an EW system to be an EW system, but these hardware systems today have significantly more inherent capabilities."

To demonstrate the concepts of multi-

capability systems, CERDEC chose not to solely focus its science and technology efforts on researching solutions to address specific cyber and EW threats, but also to develop the architecture onto which scientists and engineers can rapidly develop and integrate new, more capable solutions.

"As an example, the World Wide Web has grown into an architecture that is so powerful your tech savvy 10-year-old can build a website -- and a pretty powerful one at that," said Bertoli. "The only reason this is possible is because there is a wealth of common tools, like web browsers and servers, and standards such as HTML or HTTP already in place for them to use."

(Continued on page 40)

(Continued from page 39)

“The ICE program is attempting to extend this model to the cyber and EW community by providing mechanisms to enable the leveraging of available tactical assets to support cyberspace operation mission sets. Early focus revolves around the development of augmented situation-awareness capabilities but will evolve to include the enabling of a multitude of cyberspace operations,” said Bertoli.

ICE will provide the Army with common tools and standards for developing and integrating cyber and EW capabilities.

“Capabilities can be developed to combat EM (electromagnetic) and cyber threats individually, but this is neither time nor cost effective and simply will not scale in the long term. The domain is just too large and will only continue to expand,” said Bertoli.

“In the end, we (CERDEC) believe this is the only way the Army will be able to keep pace with the anticipated technology advancements and rate of change related to cyberspace and the systems that comprise it,” said Bertoli.

The Army acquisition community has also seen changes in the relationship between cyber and EW.

“Tactical EW systems and sensors provide for significant points of presence on the battlefield, and can be used for cyber situational

awareness and as delivery platforms for precision cyber effects to provide a means of Electronic Counter Measures and Electronic Counter-Counter Measures, for instance,” said COL Joseph Dupont, program manager for EW under Program Executive Office Intelligence, Electronic Warfare and Sensors.

“There is no doubt in my mind that we must provide for a more integrated approach to cyber warfare, electronic warfare and electromagnetic operations to be successful in the future conduct of unified land operations,” said COL Dupont.

CERDEC, as the Army’s research and development experts in cyber and EW, works closely with the Program Executive Offices, the Army’s Training and Doctrine Command and Army Cyber Command to shape operational concepts and doctrine by providing technical expertise regarding technically achievable solutions in the context of the tactical cyberspace operations and supporting materiel capabilities for the Army.

In addition to working with the Army’s strategy and policy makers, CERDEC I2WD has tapped into its facilities and pre-existing expertise to further the ICE program.

CERDEC I2WD maintains state-of-the-art laboratories that support both closed and open-air testing facilities to provide relevant environment conditions to conduct research that provides a seamless cyber-electromagnetic environment

with both wired and wireless modern communication infrastructure.

“We leverage these facilities and our inherent core competencies in cyber, EW and signals intelligence to engage with the Army and the community at large, both academia and industry partners, to collaborate on developing and integrating relevant technologies to achieve domain superiority in a changing environment,” said Robb.

The fully-instrumented labs include commercial information assurance products and allow for in-depth experimentation while sustaining automated rapid network re-configuration technology and virtualization technologies to support scalable testing. Additionally, I2WD expands its potential environment by maintaining remote connections with external government sites, which also enables collaborative experiments.

The combination of these assets and expertise allows CERDEC to demonstrate achievable capability improvements related to cyber and EW convergence.

“During the next three years, the biggest thing we can do within the ICE effort is show the ‘art of the possible’ by providing technology demonstrations on both existing and experimental Army systems to provide concrete proof of the advantages such a capability can provide,” said Bertoli.



Joint Readiness Training Center offers broadening assignment

*By CPT Vasilios Agapios
and CPT Chaz Jordan*

The Joint Readiness Training Center at Fort Polk, La. is a premier training destination that also offers one of the most rewarding, broadening assignments for a Signal officer.

A JRTC rotation is the last collective training event for a Brigade Combat Team making the combat training center the last major opportunity for the unit to train its staff as they will fight. It is therefore a culminating challenge for the BCT Signal Soldiers, one that should build a cohesive communications team. As such, it is imperative that we provide relevant and realistic training scenarios along with world-class coaching and



mentoring to ensure that units are as ready as they can be prior to deployment.

At the epicenter of the JRTC experience is the Observer Coach Trainer team which partners with the S-6 section of the rotational training

unit. As OCTs we are charged with providing the RTU with best practices, current doctrine, and vignettes from our personal experiences to make them combat ready.

Although most Soldiers would react with disdain at the thought of an assignment at Fort Polk, I would tell them to not be so quick to judge based on the installation's reputation. Most S-6s only get to experience JRTC through the stresses of a rotation.

The demanding environment and often harsh conditions leave people with a sense of relief that the rotation is over and the idea that they never want to come back to JRTC again in any capacity. However, being an OCT can be a very fulfilling career broadening opportunity.

Where else in the Army can you go and in one year see how ten different BCTs, to include National Guard units, conduct Signal operations? You not only evaluate how other S-6s perform their duties, but it also gives you an opportunity to reflect and evaluate your own



The Joint Readiness Training Center offers challenging opportunities for Signaleers to train communications teams in realistic scenarios as units ramp up for pending operations.

(Continued on page 42)

(Continued from page 41)

past performances as an S-6. As OCTs we get to experience the good, the bad, and the ugly of S-6 shop operations. And as much as we teach to the various S-6 shops, there is equally as much to learn from each rotation.

Our Signal OCT team is comprised of Officers, Warrant Officers, and senior Non-Commissioned Officers who have completed their respective key development assignments and have excelled in those assignments. OCTs are often placed in the difficult position of coaching and training their peers, and therefore must have “been there, done that” and done it extremely well if their advice is to be taken seriously. As a result, JRTC only accepts some of the best and brightest within the Signal Corps to be an OCT. Those selected to be an OCT are expected to work almost autonomously and with very little supervision.

During rotations, the Signal OCT teams become attached to their respective Task Force, mirroring the BCT construct. We have Signal team representation at Infantry and Field Artillery Battalions, Cavalry Squadrons, Aviation Battalions, as well as the Support Battalions and Signal Companies. The BCT headquarters gets its own robust Signal OCT team as well, with representation for the Help Desk, Enterprise Operations, Network Operations, Communication Security, and of course the Officer and NCO in charge.

As the real-world operational environment changes, so too does Army Doctrine. JRTC adapts its rotational situation quickly in order to keep units trained and ready for the next conflict. These are called Decisive Action Training Environment rotations and consist of the unit’s initial entry into the training area, establishing a defense, and finally offensive and stability operations. These rotations are designed according to the Army’s Operational Concept outlined in Chapter 2 of Army Doctrine Reference Publication (ADRP) 3-0 (pp. 2-2 - 2-8). With the drawdown of forces in Afghanistan, as well as mounting tensions in several countries around the world, DATE rotations are becoming more frequent than traditional rotations where the objective was to prepare a unit for a known



An instructor at the Joint Readiness Training Center gives a communications team member close support and guidance during an exercise.

deployment into a known area. Transitioning from over 10 years of operating in counter insurgency environments to a more austere and expeditionary environment can be difficult for Signal shops. As a result, Battalion and Brigade S-6s have to modify what they have learned, and in some cases completely re-learn some of the concepts they were taught regarding how units communicate. As an OCT you are the subject-matter expert in Signal doctrine and your main focus is coaching your counterpart through the roadblocks they may encounter.

We are, by the nature of the job, impartial collectors of data. We observe, green books in hand, how the units normally conduct business. These observations are the driving force behind how and what we coach to the RTU. We arm S-6 shops with current doctrinal procedures and proven tactics, techniques, and procedures for the best ways to be successful, yet also allow them the flexibility to modify and experiment with their own TTPs to test their effectiveness in a safe training environment which mirrors as closely as possible the same conditions that the unit would experience in combat situations.

Personally, the part of the job that I enjoy the most is the one-on-one coaching that I get to do with my counterpart. It is during this time that I can bring issues to light that the S-6 may not have been aware of due to being too close to the action. We then discuss ways to resolve those issues and improve the overall functionality and effectiveness of the S-6. I cannot begin to describe the personal satisfaction you feel as an OCT to watch the training S-6 shop morph and grow, through your coaching, into a highly effective combat multiplier ready to go to war.

At JRTC, the life of an OCT revolves around the rotations. But there are a lot of training opportunities outside of the rotations. Fort Polk offers a Warrior Signal University where you can take classes in preparation for civilian certifications. As a small example, there are regular offerings of the CompTIA Network+ and Security+ certification, as well as the various Cisco and Microsoft certifications. Also, since JRTC is an Airborne unit, qualified Soldiers are eligible to attend the Static Line Jumpmaster course. We also have opportunities to work with Mobile Training Teams for the Pathfinder and Air Assault courses.

As great as those education and training opportunities are, they are nothing compared to what you can learn from JRTC's Leader Development Program and the rest of the OCTs that you would work with. Between the entire Signal team, there is over 100 years of experience to draw from, and everybody brings something unique to the table. We have Soldiers with experience in working with tactical units such as the 82nd Airborne Division, 101st Airborne Division, 10th Mountain Division, and the United States Army Special Forces Command. We also have Soldiers who have worked at the strategic level in units aligned under Network Enterprise

Technology Command. This melting pot of experiences results in a well-rounded team who can call on each other to help out when we find ourselves in unfamiliar situations.

Working as an OCT has opened my eyes to a much more macro view of the Signal Regiment than I ever would have seen had I stayed focused on remaining in a single tactical unit beyond my KD time. I am thankful for the opportunity to work in this capacity and to help out my fellow Signal Officers as they prepare to put themselves and their shops through the ultimate test of deploying to a combat zone. Being assigned as an OCT at JRTC has made me a better and more rounded Signal Officer, ready for the challenges that come with future assignments.

For additional information about JRTC, go to the JRTC, Operations Group website at <http://www.jrtc-polk.army.mil/OPS/index.html> or the Signal Best Practices website at <https://www.us.army.mil/suite/page/590479>.

CPT Vasilios Agapios is a Signal OCT who works with S-6s in Infantry Battalions. He holds a Bachelor of Science degree in Information Systems Management from the University of Maryland Baltimore County and a Master of Science degree in Information Assurance from the University of Maryland University College. He has also earned the CompTIA Security+ and Network+ certifications. His previous assignment was as the S-6 for 4th Battalion, 10th Special Forces Group (Airborne) in Fort Carson, Colo.

CPT Chaz Jordan is a Signal OCT who works with S-6s in Cavalry squadrons. He holds a Bachelor of Science degree in Interdisciplinary Studies from Tennessee State University. His previous assignment was as the S-6 for 1-72 Armor Battalion, 1st Heavy BCT, 2nd Infantry Division in Camp Casey, ROK.

ACRONYM QuickScan

ADRP – Army Doctrine Reference Publication
BCT – Brigade Combat Team
COIN – Counter-Insurgency
DATE – Decisive Action Training Environment
JRTC – Joint Readiness Training Center

KD – Key Development
OCT – Observer Coach Trainer
RTU – Rotational Training Unit
TTP – Tactics, Techniques, Procedures

44th Expeditionary Signal Battalion executing mission

By CPT Christina Knight and
CPT Sean Ruddy

The future of our Signal Regiment calls for great Soldiers.

The demands of a Signal Soldier are often explicit, implied or directly derived from higher requirements. These unique requirements are imposed based on unique mission requirements and evolving technologies while others are imposed based on organizational expectations.

In 2010, in response to a 2005 Department of Defense Directive that required certification for members (civilian and military) in order for them to have privileged access to DoD Information Systems, the Chief Information Officer /G6 published a memorandum titled, "In the U.S. Army Information Assurance Military Workforce Certification Process.

This document outlines the DoD Directive 8570.1 compliance standards for Signal Soldiers in MOS 25B or 25U. The document, further mandates that Soldiers in these Military Occupation Science obtain Information Assurance Technical level I-II; they must complete industry level certification (COMPTIA A +, NETWORK

+, or Security +) on top of the base line certificates to include the 6 mandatory training such as Information assurance and thumb drive awareness. U. S. Army Europe PAM 25-2 requires that USAREUR Soldiers complete the additional certifications of Organizational Unit Administration and Windows 7 in order to be designated as unit administrators for Europe.

Certifying Soldiers to meet the DoD 8570 and USAREUR requirements is costly in both time and money. In a period of drawdown and sequestration the success stories of doing more with less are worth sharing.

The 44th Expeditionary Signal Battalion has developed a method to address the cost related issues of this requirement that might be applied to other formations by making 8570.1 compliance a priority for the signal workforce.

DOD 8570.1 is the standard to certify and train Signal Soldiers in order to obtain varying levels of technical expertise based on their position in the organization. For example, a Soldier who is positioned as an Information Assurance Technician level I is required to obtain Comptia A+ or

Network + to work in this capacity, which generally means having administrator access for machines on the network. This level of training will allow the Soldier to have basic knowledge of how the computers and devices on the network interact within the network infrastructure. This access is typical for Soldiers between the ranks of E1-E4 lacking any prior experience or training beyond their military provided education.

IAT level II requires Soldiers to obtain Comptia Security + Windows 7, and OU Administration in order to have administrative rights on the network. This level of training is typically associated with team leader (E-4 to E-5) responsibilities. These personnel should have mastered the concepts and techniques required for IAT-I. IAT II Soldiers are equipped to administratively modify the network, ensure cyber security through vulnerability management, create user accounts and computers in Active Directory, apply Security Technical Implemental Guides to all devices across the network, troubleshoot issues in hardware and software, and make remotely issued repairs to devices.

At the Battalion level, the

highest technician and IT manager is the Information Assurance Manager level II, and is held by the Captain and/or Warrant officer in the S6 office. They are responsible for the IA program for Information Systems within the Joint Network Environment. Personnel in these positions perform a variety of security related tasks, including the development and implementation of system information security standards and procedures. They ensure that IS are functional and secure within the JNE. They are also responsible for the management and tracking of all the personnel who need to meet the 8570.1 M standards to perform the required job.

The traditional option for compliance is to go through AE-ITT, Mobile Training Teams teams from Fort Gordon, or to send Soldiers to school for the training. For the 44th Expeditionary Signal Battalion, which operates in USAREUR, the OU admin requirement involves a two day course about 30 min from home station and requires Soldier to either obtain a ride or take the bus to and from the testing center. The course and the admin test cost \$185.55 per Soldier. The Windows 7 training, also required in USAREUR, can either be obtained online or through a five day course. As with the OU Admin, this course is thirty minutes away for Soldiers and costs the unit

\$1,057.85 for each Soldier to attend the course. The Comptia certifications (mainly Security +) is a industry level certificate that requires an outside instructor to fly in from the states and give a 40 hour block of instruction costing the unit \$808.55 per Soldier. The final step is getting a voucher after completing all Skillport requirements which costs \$275.00. The total cost per Soldier is 12 days away from mission requirements and \$2,315.95. These figures in time and money are extremely costly among large formations such as the 44th ESB. The Army maintains a high dollar amount specifically for individuals to be trained in a unit; this funding is no different than for aviators to go into simulation training.

Although the money is mandated to be allocated, but units are able to drastically reduce the cost for DoD wide by providing local level training. These mandatory requirements are not met in the schoolhouse, but instead are each unit's responsibility

to complete once a Soldier has arrived. The 44th ESB's goal was to have all Signal Soldiers DoD 8570.1 compliant and not just 25Bs or 25Us; a review of available signal Soldiers in the unit of all Signal MOSs identified 308 Soldiers and Officers needed to complete the requirements. According to AE-ITT standardization, the total cost to train the battalion would be \$713,620.60.

The 44th ESB recognized the inefficiency of this method, especially as it faced a military drawdown, budget constraints, furloughs and sequestration. Company commanders worked as a team to find alternate methods to train the Soldiers and obtain their DoD 8570.1 compliance at a lower cost in both time and money.

The 44th ESB established a local training center and used Soldiers as subject matter experts to teach the classes. This training center consists of a 14 station computer lab, conference area for teaching, and

(Continued on page 46)

AE-ITT Cost			44th ESB Cost		
Course	Time period	Cost	Course	Time period	Cost
Windows 7	5 Days	\$1,047.85	Windows 7	40 hours	\$0
OU Admin	2 Days	\$185.55	OU Admin	1 Day	\$0
SEC+ Course	5 Days	\$808.55	SEC+ Course	40 hours	\$0
Voucher	none	\$275.00	Voucher	None	\$27
Total	12 Days	\$2,316.95	Total	Mission dependent	\$27

Figure 1: Cost/ Time comparison of AE-ITT vs. 44th ESB

(Continued from page 45)

electronic whiteboard. This allows leaders to assess their Soldiers and send them to their next appropriate training requirement, test out of a requirement, or use the lab for Skillport training. Establishing this facility in conjunction with using trained Signaleers drastically reduced cost and time to train Soldiers.

The following diagrams illustrate the cost and time associated through AE-ITT method vs. the 44th ESB method:

The difficulty facing commanders is having a large number of Soldiers who do not meet an Army directed training requirements.

Although the school house does not filter the Soldiers who are unable to complete the mandatory training, commanders can use the BAR to re-enlistment as a tool. Meeting and enforcing the demands of today's IA requirements are critical for the current Internet environment.

It is a commander's job to ensure that they train Soldiers and retain the best who meet the standard. A Soldier will be given a suitable amount of time to complete the Skillport training, attend the class and receive a voucher. If a Soldier is unable to pass the mandatory examination the commander has the authority to BAR the Soldier and give them another opportunity to take the exam



ATCTS-8570 IT-II



	SEC+ Skillport 301+ Training Completed	AE-ITT Security + Class OR Schoolhouse Completed	Security + Certificate	Needed for SA Rights		Fully SA Qualified	Holds ASCL Card
				OU Admin	Windows 7		
HHC	12	12	12	8	15	8	6
A	78	53	30	44	71	31	19
B	77	37	33	59	72	34	15
C	40	17	15	33	28	15	3
BN Total	206	1119	90	144	186	88	43

Figure 2: 44th ESB 8570.1 compliance standings

to overcome the BAR or the Soldier can re-class, or be separated from the Army.

Over the past year, The 44th ESB has continued to make significant in DoD 8570.1 certification. Over 119 Soldiers and Officers completed the requirements at a rapid and economically feasible pace using our locally developed program.

Army leaders continue redefining the process and applying appropriate training for certain skill sets and MOS. As the focus on the cyber security continues expanding, the Soldiers engaged in the cyber fight need to be well trained and proficient in those tasks. Evolving threats necessitate an understanding that all requirements cannot be taught at the schoolhouse. The responsibility for on-the-fly training rests with unit leaders.

Completing this essential training can be overwhelming based on budget and time constraints but failing to

complete the training is not an option. The Network is a weapon system operating under specific DoD 8570 guidance standards. Enforcing this standard is critical for Signal leaders so that all our forces can maintain network security.

Professionals in the 44th ESB have sought out opportunities to provide training at low cost and flexible times according to the individual unit's mission requirements. The training and certification demands of the DoD on our Regiment will continue to increase as we provide "The voice of freedom."

Efficient networks have been part of our reputation and efficient training methods need to be shared and continued.

CPT Jacob Roecker, CPT Zachery Landis, CPT Steve Robitaille and CPT Sharon Manning contributed to this article.

CPT Christina Knight earned a BS degree in Criminal Justice and was commissioned through the Reserve Officers' Training Corps of Seton Hall University in 2007. CPT Knight holds a Master of Science degree in Administration from Central Michigan University. Her assignments include platoon leader, executive officer in Bravo Company 45th Combat Support Battalion and 45th Sustainment Brigade. She completed the Signal Captains Career Course and the Battalion Signal Officers Course.

CPT Sean Ruddy earned a BA degree in Psychology and was commissioned through the Reserve Officers' Training Corps of Arizona State University in 2007. He completed Signal Officer Basic Course at Fort Gordon, Signal Captains Career Course and the Functional Area 53 (FA53) Course. He is currently serving as battalion Information Assurance officer for the 44th Expeditionary Signal Battalion.

ACRONYM QuickScan

CIO/G6 - Chief Information Officer
DoD - Department of Defense
ESB - Expeditionary Signal Battalion
IA - Information Assurance
IAM - Information Assurance Manager
IAT - Information Assurance Technician
IS - Information Systems

JNE - Joint Network Environment
MOS - Military Occupation Science
OU - Organizational Unit
PAM - pamphlet
U.S. - United States
USAREUR - United States Army Europe

New field support model implemented

By Richard Licata

Professionals in the Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance community are pioneering a new field support construct that will transition a decade's worth of contractor-developed knowledge into the hands of the Soldiers.

This four-tiered model, which redefines roles and maintains Soldier access to specialized subject matter experts, will be implemented across Combat Training Center rotations and home station training exercises between fiscal years 2014-2015. Already piloted at multiple rotations at the Joint Readiness Training Center, Fort Polk, La., and National Training Center, Fort Irwin, Calif., the new model emphasizes the importance of knowledge transfer from contractor and organic field support personnel to Soldiers. It is designed to equip Soldiers with the basic skills needed to resolve low-level issues in the field along with multifunctional embedded support, while simultaneously reserving specialized reach-back support and providing tools that will track trends and adapt field support surge packages as needed.

BG Dan Hughes, program executive officer for Command, Control and Communications-Tactical, said this effort presented an opportunity to direct an "investment back into Soldiers and help them keep pace with ongoing deployment of the C4ISR systems required for mission success. Evolving our field support also aligns with the overall Army effort to simplify these systems for the end-user."

The Team C4ISR Field Support Integrated Process Team developed the new field support construct in coordination with professionals from the U.S. Army Communications-Electronics Command Logistics Readiness Center and Software Engineering Center; Tobyhanna Army Depot, Pa.; PEO Intelligence, Electronic Warfare & Sensors and PEO C3T.

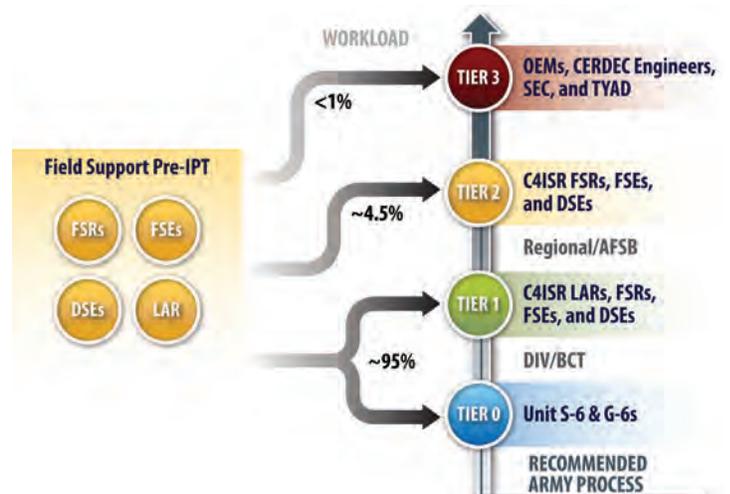
The new model prescribes that if Soldiers are unsuccessful at troubleshooting issues,

they can escalate a trouble ticket to a tier 1 team of multifunctional logistics assistance representatives, digital systems engineers or select field support representatives for mission critical or high-density systems. This multifunctional team possesses the capability to cover all C4ISR weapon systems in the field, and each member is aligned to a specific weapon system or group of weapon systems based on skill set requirements.

If resolution is unattainable, the appropriate system-specific subject matter experts at tier 2 will attempt to resolve the issue primarily through remote or telephonic support, and if needed, pass to tier 3 engineers to determine a hardware/software modification, as the problem is most likely unique.

Through site visits and thorough reviews of trouble tickets, the IPT launched an extensive analytics initiative to produce a model that incorporates feedback from Soldiers at training rotations and that has been validated across multiple units. The IPT's approach integrated quantitative data pulled from more than 10,000 field support trouble tickets, as well as qualitative observations from multiple home station visits to develop its new field support construct.

It determined that 78 percent of all trouble tickets recorded between the pilots and validation exercises at both JRTC and NTC



were training related, and could be resolved at a lower echelon had training been performed at home station prior to the rotations. Further, home station Mission Command Systems Integration Training events at Fort Hood, Texas, and Fort Drum, N.Y., showed that contractors were conducting battlefield circulation and handling a majority of issues that Soldiers could resolve internally, through the application of some training.

“The bottom line was that we were able to see a missed opportunity,” said Gary Salomon, associate director for Programs, CECOM Logistics Readiness Center. “Units relied heavily on contractor field support, even to address the most simplistic of problems, so the IPT came up with a new structure to deliver Soldiers the basic skills they need to expedite quick fixes and the right mix of embedded and reach-back support.”

The tiered structure is Soldier-tested and validated. A control exercise was completed at a recent JRTC rotation, during which the IPT monitored

TIER 1 PERSONNEL	SYSTEMS
1 - DSE	CPOF, AFATDS, BCS3, Command Web
1 - FBCB2/BFT	FBCB2 platform, EPLRS, JCR, TIGR
1 - EPLRS	FBCB2 platform, EPLRS, JCR, TIGR
1 - DCGS-A/DTSS	DCGS-A, DTSS, TGS, Prophet, Trojan
1 - MC Server (TMC BCCS)	Mission Command Servers
1 - CHS	CHS
1 - TOC/PPP	ADAM
1 - CECOM SENSOR	Multifunctional: Firefinder, Prophet, Trojan, Profiler, TGS, GBS, LCMR
1 - CECOM IT RADIO	Multifunctional: Tactical Radios, GBS, NVGs, DAGR, TOCS, SWIC-3/5, CS-13/14
1 - CECOM AVIONICS	Multifunctional: Aircraft Communications, Navigation, Sensors, RADAR, ATC equipment
1 - CECOM IT SWITCH	Multifunctional: JNN, SSS, BnCPN, HUB, TCN, JGN, BVTC, NetOp
1 - CECOM LHT	Multifunctional: Phoenix, TACSAT, STI, SNAP, TROPO, HCLCS
1 - CECOM P&E	Multifunctional: Power Generation/distribution systems & Environmental Control Units
1 - CECOM IT LOG	Multifunctional: SAMS-1E(V)2, CSS-VSAT, TC-AIMS II, MTS

the implementation of the tiered construct and collected data in the background. The JRTC Operations Group took full ownership of the construct and successfully implemented lessons-learned from the pilot exercises. The unit took recommendations provided by the IPT and JRTC, and allowed a surge support package of tier 1 and 2 personnel to conduct battlefield circulation during the brief Reception, Staging, Onward Movement and Integration phase of the exercise. The surge period allowed the unit to rapidly set-

up, validate its C4ISR systems and conduct the Force on Force portion of the exercise with little external support. The IPT allowed the unit to complement the tier 1 support package with two additional personnel.

The C4ISR Field Support IPT projects that phased reductions will reduce costs 20 percent annually over the next two years and an additional 20 percent over the fiscal years 2016-2019 Program Objective Memorandum.

The IPT leadership notes that continued partnership with AMC, FORSCOM and the Training and Doctrine Command, as well as ASA(ALT), will be integral to the success of end to end implementation of the tiered structure and supporting initiatives.

Richard Licata is the PEO C3T field support optimization chief and co-lead of the C4ISR Field Support Right-sizing IPT. He holds a B.S. in organizational management from Wilmington University, is Level III certified in program management and is a certified Lean Six Sigma Black Belt.

ACRONYM QuickScan

AMC – U.S. Army Materiel Command
ASA(ALT) – Assistant Secretary of the Army for Acquisition, Logistics and Technology
C4ISR – Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance
CECOM – U.S. Army Communications-Electronics Command
DSI – Digital systems engineer
FORSCOM – U.S. Army Forces Command

FSR – Field Service Representative
IPT – Integrated Process Team
JRTC – Joint Readiness Training Center
LAR – Logistics assistance representative
NTC – National Training Center
PEO C3T – Program Executive Officer for Command, Control and Communications-Tactical
POM – Program Objective Memorandum
TRADOC – U.S. Army Training and Doctrine Command

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

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

OFFICIAL BUSINESS
ISSN 0362-5745



Celebrating an updated landmark at Gate 1 are: Augusta Mayor Deke Copenhaver, left; MG LaWarren Patterson, U.S. Army Cyber Center of Excellence and Fort Gordon Commanding General; CSM Ronald S. Pflieger, Cyber Center of Excellence Command Sergeant Major; CSM Kenneth Stockton, Fort Gordon Garrison Command Sergeant Major; Nelson Keeler, U.S. Army Cyber Center of Excellence and Fort Gordon Deputy to the Commanding General; and COL Samuel Anderson, Fort Gordon Garrison Commander.

Physical changes in and around Fort Gordon herald a transformation to meet the Army's expanding role in cyberspace operations.

While the new Cyber Center of Excellence is evolving, see in the next issue how the Signal Regiment is radically changing to function seamlessly in this new environment.

**ARMY
COMMUNICATOR**

Signal Towers, Room 713
Fort Gordon, Georgia 30905-5301
PIN: 104263-000