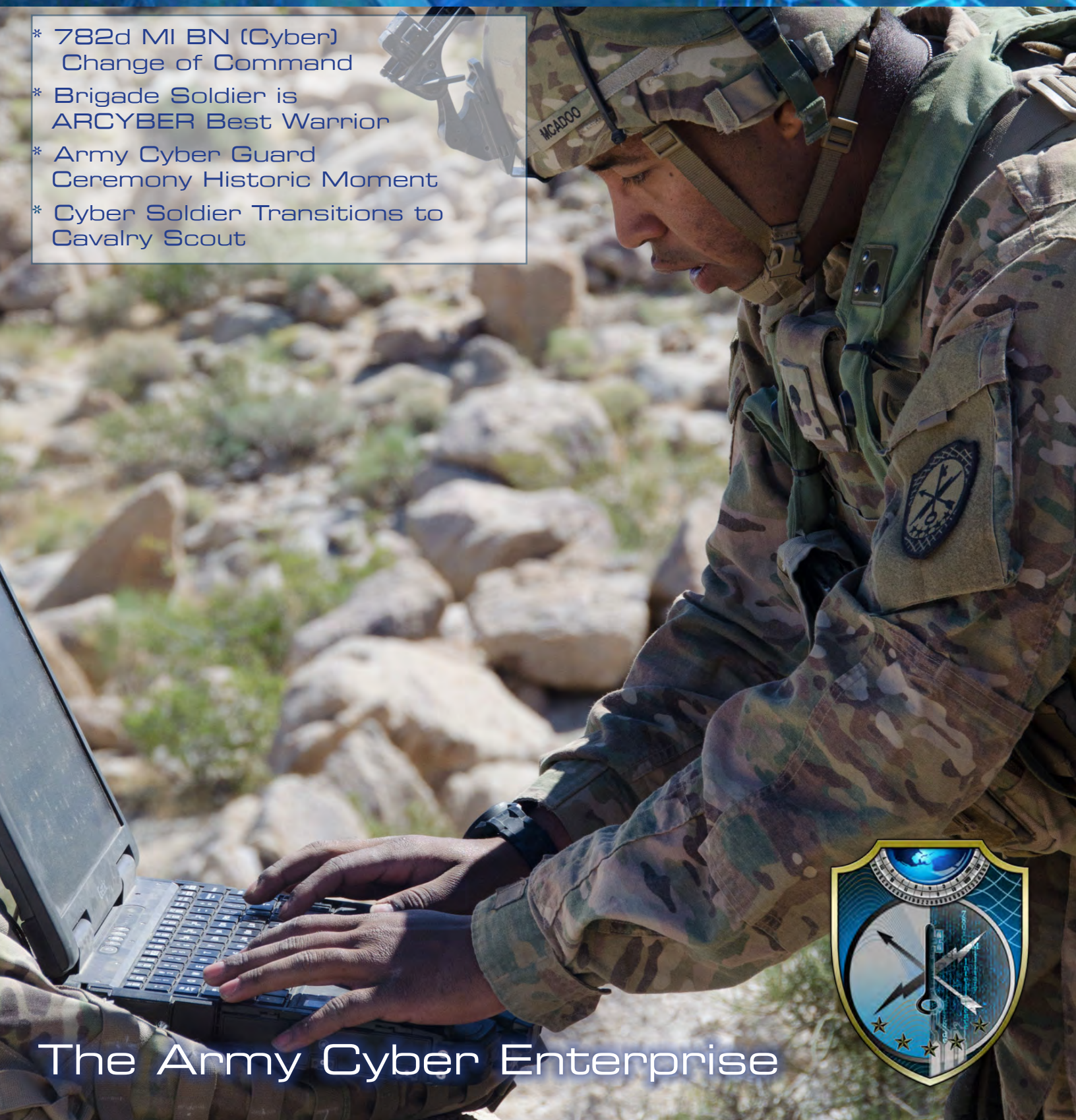
Volume 5, Issue 4

the BYTE

780th Military Intelligence Brigade

* 782d MI BN (Cyber) Change of Command
* Brigade Soldier is ARCYBER Best Warrior
* Army Cyber Guard Ceremony Historic Moment
* Cyber Soldier Transitions to Cavalry Scout



The Army Cyber Enterprise

The BYTE is a publication of the 780th Military Intelligence (MI) Brigade, Fort George G. Meade, Md.

The BYTE is an official command information publication authorized under the provisions of AR 360-1. The magazine serves the service members and civilians of the 780th MI Brigade and their Families.

Opinions expressed herein do not necessarily represent those of 780th MI Brigade or that of the Department of the Army.

All photographs published in the BYTE were taken by 780th MI Brigade Soldiers, Department of the Army Civilians (DACs), or their Family members, unless otherwise stated. The front cover and graphic posters contained within the BYTE were created by the previous Brigade public affairs officer (PAO), Tina Miles, or Steven Stover, unless otherwise stated.

Send articles, photographs or story ideas to the 780th MI Brigade PAO at steven.p.stover.civ@mail.mil, or mail to 310 Chamberlin Avenue, Fort George G. Meade, MD 20755.

For additional information, call (301) 833-6104.

Col. John "Dave" Branch
Commander

Command Sgt. Maj.
Sheldon W. Chandler Jr.
Command Sergeant Major

Steven Stover
Public Affairs Officer
and Editor

'80MIB QRCode.pn(

COLUMNS:

In every issue...

On the cover: Spc. Steve McAdoo, a cyber network specialist with the 780th Military Intelligence Brigade, sets up cyber tools overlooking the city of Razish at the National Training Center at Fort Irwin, Calif., May 5. (photo by Bill Roche, U.S. Army Cyber Command)

FEATURES:

ARTICLES:

the BYTE: INSCOM's nominee for the 2015 Maj. Gen. Keith L. Ware Public Affairs Competition.
The annual Department of Army's competition recognizes Soldiers and DA Civilians for excellence in achieving the objectives of the Public Affairs Program.

From the Editor

The Collin English Dictionary defines an "Enterprise" as a company or business; something new, difficult, or important that you do; *and* the ability to think of new and effective things to do, together with an eagerness to do them.

The theme for this issue is the *"Army Cyber Enterprise"* – collectively, the 780th Military Intelligence Brigade, the Cyber Protection Brigade, and 1st Information Operations Command are the U.S. Army Cyber Command's (ARCYBER) operational arms of the Army Cyber Enterprise, and the Cyber Center of Excellence is the institutional arm. Together these units form the foundation for the Army's Cyber Enterprise.

The "Army Cyber Enterprise" encompasses thousands of Soldiers, DA Civilians, and contractors who are engaged in a joint and integrated venture. Together, we are embarking into a new and contested domain. We are, collectively, cyber pioneers and visionaries, and we have a singular purpose -- a purpose spelled out in the ARCYBER mission statement:

To direct and conduct integrated electronic warfare, information and cyberspace operations as authorized, or directed, to ensure freedom of action in and through cyberspace and the information environment, and to deny the same to our adversaries.

Our teams are "Everywhere and Always…In the Fight" serving under four commands and a National Command Authority; we support each of the Services; and we actively fight alongside our Joint partners to achieve U.S. supremacy in an increasingly contested cyberspace domain and electromagnetic spectrum (U.S. Army foundational theme Multi-Domain Battle).

v/r,
Steve Stover
Public Affairs Officer
780th MI Brigade
Editor, **the BYTE**

The Army Cyber Enterprise

By: Col. Dave Branch, commander, 780th Military Intelligence Brigade (Cyber)

Teammates, we are part of an Enterprise – the Cyberspace Enterprise, the Army Enterprise, and the Defense of the Nation Enterprise. In the previous **BYTE**, our focused articles centered on *Unity of Effort* – a continuously critical factor for collective success in cyberspace. My thoughts as your commander continue along that line as we transitioned personnel throughout the summer season, welcomed the Task Force Echo members to our ranks, and established a provisional Developer formation properly named Cyberspace Solutions Development Detachment. Recently, the ARCYBER CG (commanding general, U.S. Army Cyber Command) declared 2018, as "The Year of Delivery." I would say we have well and faithfully postured 780th to meet his vision and intent. Not only in 2017, but over the past six years, the brigade and the entire cyber enterprise mission has increased in scope, scale, and complexity. It is our duty to continue progressing.

In recent readings, I ran across two key Aristotle quotes relevant to our Enterprise efforts:

First, as professionals: ***"We are what we repeatedly do. Excellence, then, is not an act, but a habit."***

Secondly, and important as teammates: ***"The whole is more than the sum of its parts."***

The first quote follows our Army tradition of "Be, Know, Do" and reminds us why we train as individuals and collectively and then certify our efforts. The second expresses the concept that individuals (or individual units) when connected to form one entity are of greater worth (effectiveness) than if the individuals remain in silos. We have proven this concept a few times over now in small or specific venues such as the CEMA (Cyber Electromagnetic Activities) cell efforts supporting the tactical National Training Center rotations, in Joint Task Force Ares and the Task Force alignments of the Cyber National Mission Force (where Offensive and Defensive Cyber Operations flourish together) as well as the Joint Mission Operations Center (JMOC) integration of 1st Information Operations Brigade personnel and of highly-trained TF Echo troops (unified with us from seven states). If we "repeatedly do" this, then great habits will form and our duty of habitual progress will be achieved!

As the operational force, progress must be driven by, with and through our actions. Much like other enterprises, the future will be built on how we apply knowledge of the past and actions in the present. Each of you brings a unique knowledge, perspective, and vision that develops the formations, operations and lessons learned during our evolution. Our collective gains will inform the larger enterprise and posture commands such as the Cyber Center of Excellence, ARCYBER, U.S. Cyber Command and even partner nations to adopt and adapt. In short, yours are the shoulders that others will stand upon.

My charge to each 780th member as you read this unique BYTE and engage across the Cyberspace Enterprise is this: ***FORM THE RIGHT HABITS and CONTRIBUTE TO THE WHOLE.***

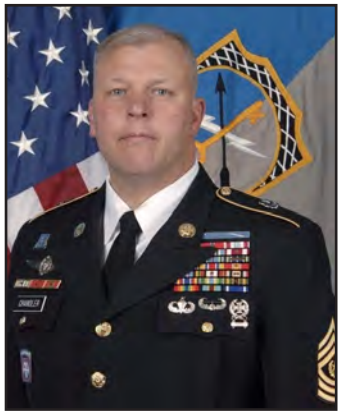
By so doing, you will remain...

Everywhere and Always….. In the Fight!

Pictured (left to right) *Col. Adam Volant, commander, Task Force Echo (TFE), Col. Dave Branch, commander, 780th Military Intelligence (MI) Brigade, Command Sgt. Maj. Sheldon Chandler, 780th MI Brigade, and 1st Sgt. Christian Smith, TFE. (U.S. Army Photo)*

Farewell: State of the Cyber Enlisted Corps

By: Command Sgt. Major Sheldon Chandler



In August of 2015, I departed Joint Base Lewis-McChord (JBLM) to make the trek across the United States to my home state of Maryland. This was the start of the most rewarding experiences in my professional career. Shortly after arriving I assumed responsibility for the most technical and forward leaning units that I have ever had the pleasure to lead in my career.

Over the last two years, it has been my absolute honor leading the Soldiers and Civilians of the 780th Military Intelligence (MI) Brigade. The efforts of the men and women across the entirety of the Brigade has made a mark on the evolution of cyberspace for our Army and our Nation. The Soldiers and Civilians of the 780th MI Brigade have played a direct role in building sound processes in cyberspace through shaping policy decisions at the Department of the Army level. To witness firsthand the tremendous growth in capabilities and the operational capacity of the brigade has been a highlight of my career. The evolution of the Army's decision to create a new cyber MOS (military occupational specialty), TRADOC (U.S. Army Training & Doctrine Command) standing up a world class Cyber School, and being part of operationalizing the newest warfighting force in our Army has been an experience that I will never forget. The Cyber Branch and its Soldiers are changing the way that we fight on the modern battlefield, but it would not at all be possible without the hard work and dedication of the many enabling functions that set the conditions for us to fight and win in cyberspace. The intelligence, signal, logistical, and administrative enablers that we have resident in the Brigade are some of the most well rounded and technically proficient Soldiers and Civilians that we have in our Army.

As many of you know, throughout my time as the Brigade Command Sergeant Major, I have traveled just a little bit. In total somewhere around 80 TDYs (Temporary Duty) and 250,000 sky miles to conduct battlefield circulation, site visits, conferences, training exercises and key leader engagements across our Army. Each one of these trips was a very unique and exciting experience as I had the pleasure to interact with the entirety of the force. During every visit I was amazed with the new solutions that our Soldiers and Civilians were creating to solve some of the most complex problem sets our Army has ever faced. Executing 3D printing to enhance drone flight, fabricating devices to survey the 802.11 environment, writing code, integrating cyber capacity into Brigade Combat Teams across our Army, networking new and enhanced operations centers, professional development opportunities, or driving change in Army policy. At the foundation of each one of these activities was a young Soldier, Warrant Officer, Officer, or Civilian who had observed a complex problem and developed a solution to enhance the cyber force and unit capabilities. Each senior Army and DoD leader that I have had the pleasure to engage during my extensive travels has consistently echoed the same message….the professionalism, talent, and tremendous capabilities of the Soldiers and Civilians in the 780th MI Brigade are superb! I appreciate your hard work and dedication to making the mission and the unit a success.

As I stated in the beginning of this article, I made the trek from JBLM to my home state of Maryland. After 26 years in the U.S. Army, my family and I have made the decision to retire from the Army and remain in place locally. Our Army career has been a superb experience and we have truly enjoyed making friends at each location along our journey. I cannot think of a greater experience to end our journey than have served in the 780th MI Brigade as your Command Sergeant Major. I am honored to have served with you and truly appreciate your hard work, dedication to duty, and service to our Army and the Nation.

Everywhere and Always….. In the Fight!

Enabling Individual Potential

By: Gregory Platt, senior civilian advisor, 780th Military Intelligence Brigade (Cyber)

FORT GEORGE G. MEADE, Maryland – Greg Platt, senior civilian advisor for the 780th Military Intelligence (MI) Brigade held a professional development (PD) for the civilian workforce on July 28 in the brigade annex. (U.S. Army Photo)

I recently hosted a seminar which focused on communication and individual professional growth. During the session we spent time discussing the Brigade philosophy of "Enabling Individual Potential" (EIP) and how creating a personal career vision statement can provide a path to guide your professional growth. Many of you contributed your thoughts on what EIP means to you in context of the brigade and while there were several terrific responses I wanted to reiterate what one of your teammates shared.

"Enabling Individual Potential is the result of creating an environment that supports individuals in the workforce to work for themselves to achieve goals. Cultivating an effective and efficient workforce requires opportunities from the employer as well as a desire and a drive from the employee. The balance in this relationship is where the 'enabling' is to take place. Only in a communicative, collaborative relationship can an employee reach their potential, and by extension, the employer can reach theirs."

Note the shared responsibility between individual and supervisor and the following key words: goals – opportunities – reach potential.

This same partnership was highlighted by the Honorable John McHugh, former Secretary of the Army, in comments he made for his Army Civilian Workforce Transformation initiative. He stated "I hold each Army Civilian accountable for mapping and navigating a progressive program of self-development. Leaders at all levels share responsibility for enabling Army Civilian employees to reach their full potential."

Reaching your full potential starts with you! It calls for introspection and honesty with yourself about what you want to accomplish in your career and in life. It requires candid conversation with supervisors, family members, and mentors – all of whom can enable you along the way. It is my intent to encourage you in the upcoming fiscal year to create your personal vision, make a plan of action – add it to your Individual Development Plan (IDP) and work with your supervisor to make it happen.

Remember, you are all members of the Profession of Arms, called upon to be Adaptive; Responsive; Ready; and Committed. Are you ready to rise to the challenge?

Be all that you can be!

FORT GEORGE G. MEADE, Maryland – Greg Platt, senior civilian advisor for the 780th MI) Brigade leads a group activity during a professional development (PD) for the civilian workforce on July 28 in the brigade annex. (U.S. Army Photo)

Cross Pollination of the Cyber Force

By Sgt. Maj. Jesse C. Potter, operations sergeant major, 780th Military Intelligence Brigade (Cyber)

On a hot and humid morning in August the historic first steps of the Cyber Branch were taken by a group of Subject Matter Experts (SMEs) at Fort Meade. Prior to the creation of the Cyber Branch, if you asked who conducted Cyberspace Operations you would get two distinct and very different answers. Signal (CMF 25) and Military Intelligence (CMF 35) Soldiers would both say that they conducted Cyberspace Operations; however, as history will show us, Signal Soldiers conducted Defensive Cyberspace Operations (DCO) while their Military Intelligence (MI) brethren conducted Offensive Cyberspace Operations (OCO). This approach was unique to the Cyber Mission Force, while enabling a rapid build of the Cyber Mission Force Teams it prevented the establishment of a viable Career Management Field and subsequent unified approach to Cyberspace Operations.

The initial approach from 2008 was refined by the Department of the Army in June 2014, who directed U.S. Army Training and Doctrine Command (TRADOC) to analyze the need for a new Career Management Field for Cyberspace Operations. The Cyber Center of Excellence (CCoE) responded to TRADOC with a proposed career force strategy that effectively and efficiently tailored existing Signal and MI capabilities to meet emerging cyberspace threats.

After 45 days of intense deliberations the SME panel recommended the establishment of the Cyber Branch, the Military Occupational Classification and its proposed structure. The subsequent approval by the Chief of Staff of the Army (CSA) ensured the Cyber Mission Force's formation, in accordance with his key directives and those of the commander for U.S. Cyber Command (CYBERCOM). However, with the establishment of the Cyber Branch, the current Cyber Mission Force structure is unable to provide synchronized and integrated Offensive and Defensive Cyberspace Operations. This difficulty is further exasperated by individual Soldiers expertise, training, and mission (OCO/DCO) alignment. To build and leverage the expertise of the Cyber Force of the Future requires an extensive hands-on approach to facilitate a cross pollination of the Cyber Force Soldiers.

Cross-pollination according to dictionary.com means "a sharing or interchange of knowledge, ideas, etc., as for mutual enrichment". In the context of the Cyber Mission Force, it is the interchange of Soldiers with specific DCO and OCO skill sets -- who are fully trained and certified with extensive background in their distinct areas of expertise. Cross-pollination of expertise is now beginning with the movement of key leaders between the two specialties. The success of this approach will be crucial in building the cyber force of the future and will require two distinct efforts.

The first approach is to understand and leverage the similarities of OCO and DCO. The second approach is to understand where they are different and have the SMEs shape cross pollination efforts. During the June 2017 Work Role Working Group (WRWG), I proved this point, surprising many of the work role care takers. Using the CYBERCOM KSAs, I removed the titles and references to the work role and then had the SMEs inform me what work role they were looking at. Every time, without fail, the offensive work roles were identified as defensive and the defensive work roles were identified as offensive.

...without fail, the offensive work roles were identified as defensive and the defensive work roles were identified as offensive.

This quick drill was later vindicated when all of the KSA were cross walked and the caretakers found that the two primary DCO work roles mapped to their OCO counterparts: Systems Analysis to DNEA\ EA\ ION – 83% similar and Network Analysis to DNEA\ EA\ ION – 75% similar. The final effort of the first approach to facilitate the cross pollination of the KSAs is a joint effort between the cyber brigades, U.S. Army

Continued on page 35

Soldiers Vie for Top Honor in INSCOM Best Warrior

By: Steve Stover, public affairs officer, 780th Military Intelligence Brigade (Cyber)

FORT GEORGE G. MEADE, Maryland – Spc. Johnny Long, left, Detachment Hawaii, 782nd Military Intelligence (MI) Battalion, was the best warrior Soldier, and Staff Sgt. Humberto Gutierrez, Headquarters and Headquarters Company (HHC), 780th MI Brigade, was the best warrior NCO following the INSCOM North Region Best Warrior Competition in May. (U.S. Army Photo)

Representing not only his command and its soldiers, Staff Sgt. Humberto Gutierrez was equally proud to showcase the prowess and professional expertise of cyber operations Soldiers who directly support the point of the spear. Gutierrez, Headquarters and Headquarters Company, 780th Military Intelligence (MI) Brigade, and Spc. Johnny Long, Detachment Hawaii, 782nd MI Battalion, 780th MI Brigade, will represent their region in INSCOM's Best Warrior Competition (BWC) in July.

Gutierrez and Long came out on top as the best non-commissioned officer and Soldier, during the north region competition held at Fort Meade and Gunpowder Military Reservation, Glen Arm, Md., May 8-12.

The top NCO and Soldier competitors from the 1st Information Operations Command (Land), 704th Military Intelligence (MI) Brigade, 780th MI Brigade, 902nd MI Group, Army Field Support Center, Army Operations Group, and Headquarters & Headquarters Company, INSCOM, completed five days of rigorous testing in numerous events including an Army Physical Fitness Test, a panel board, a written exam and essay, M9 pistol and M4 rifle weapons qualification, day and night land navigation, a 12-mile road march with a stress shoot exercise, Army Warrior Tasks and Battle Drills, an obstacle course, and a functional fitness event.

According to Sgt. Major Craig Hood, the operations sergeant major for the 704th MI Brigade, although only one Soldier and NCO advanced to the next level of the competition, all the competitors and their sponsors are winners.

"Ultimately, there is going to be one Soldier and one noncommissioned officer selected to move forward," said Hood. "But at the end of the day they will all be winners because this event tested them, physically and mentally, and these skill sets will translate onto the battlefield."

Long, the INSCOM North Region's Best Soldier, was ecstatic when he won, but also felt an obligation to the other competitors and their commands to win at the

GLEN ARM, Maryland – Staff Sgt. Humberto Gutierrez, HHC, 780th MI Brigade, fires his M4 rifle as part of a stress shoot event during the INSCOM North Region Best Warrior Competition at Gunpowder Military Reservation, May 10. (U.S. Army Photo)

GLEN ARM, Maryland – Staff Sgt. Humberto Gutierrez, HHC, 780th MI Brigade, throws a smoke grenade to mark a helicopter landing zone in order to evacuate a casualty, an Army Warrior Task, as part of the annual INSCOM North Region Best Warrior Competition at Gunpowder Military Reservation, May 10. (Photo credit: Staff Sgt. Shawn Cassatt, 704th Military Intelligence Brigade)

subsequent level.

"All the competitors came here with the same mindset, with the same goal in mind," said Long. "We went all out, but for fun, pushing each other. It's been a crucible experience because of how hard we pushed each other… and now I have a lot of work to do. It's going to be an interesting road."

Gutierrez, the INSCOM North Region's Best NCO, felt the level of competition helped everyone push harder. He was also proud to be able to represent the Army's newest military occupational specialty, 17C. The cyber operations specialist MOS was only recently established in October 2015.

"Being chosen as the NCO best warrior means a lot to me and my unit," said Gutierrez. "To see a cyber Soldier going up to the INSCOM level is special."

For the wining competitors, their journey isn't over yet. Both realize there is more fitness training and studying to do in preparation for the next level of competition; however, until then, their command is proud of them.

"Staff Sgt. Gutierrez and Spc. Long have distinguished themselves not only as the best of the best in the 780th MI Brigade but also across four other Major Subordinate Commands in INSCOM," said Command Sgt. Maj. Sheldon Chandler, the senior enlisted leader for the 780th MI Brigade. "I am extremely proud of their level of professionalism, dedication to excellence, and the warrior spirit they displayed during such a mentally challenging and physically grueling competition."

GLEN ARM, Maryland – Spc. Johnny Long, Detachment Hawaii, 782nd Military Intelligence (MI) Battalion, 780th MI Brigade, completes a 12-mile ruck march as part of the annual U.S. Army Intelligence & Security Command North Region Best Warrior Competition at Gunpowder Military Reservation, May 10. (U.S. Army Photo)

Process is Easy. Culture is Hard.

By: Lt. Col. Justin Considine, commander, 781st Military Intelligence Battalion (Cyber)

What if you could combine the adaptability, agility, and cohesion of a small team with the power and resources of a giant organization? ~ General (Ret.) Stanley McChrystal

Recently, I had the opportunity to participate in the 2017 Army Intelligence Industry Day sponsored by the Armed Forces Communications & Electronics Association (AFCEA), hosted by the Department of the Army G2 (Intelligence), and chaired by the Program Executive Office for Intelligence, Electronic Warfare & Sensors (PEO IEW&S).

Invitees to the daylong event included prominent acquisition and development organizations from across the Department of Defense and numerous public and private sector industry partners. On behalf of the brigade commander I was asked to participate in the Electronic Warfare & Cyber panel led by Maj. Gen. Patricia Frost, director of the Cyber Directorate and principal staff advisor to the Chief of Staff of the Army (CSA) and Secretary of the Army for cyberspace operations, electronic warfare and information operations.

Alongside U.S. Army Training & Doctrine Command (TRADOC) Capability Managers (TCM), the Program Manager for Electronic Warfare/Cyber, and an Intelligence & Information Warfare Directorate (I2WD) representative, I felt my role was to present the cyber warfighter's perspective in a high-level enterprise discussion on the current state of the Nation's ability to 'maintain relative advantage, adopt disruptive technologies, and adapt best of breed commercial technologies' – the overarching theme of the event. In that role, the image in my mind resembled WWI trench warfare – an embattled commander being asked 'how can we help?' as he is leading courageous Soldiers desperately outmanned, out-gunned and out-matched – but perhaps worst of all… out-empowered.

If an "enterprise" can be defined as a difficult undertaking requiring organizational adaptation and intellectual innovation, and the Army Cyber Enterprise encompasses an integrated venture of cyber pioneers and visionaries (read: Vanguard) ~ we must likewise acknowledge that our center of gravity is cultural, not technical. As noted during the Industry Day, we are failing in three critical aspects: trust, risk acceptance, and a sense of urgency.

"Leaders must value trust and empowerment"

Despite the quantifiable fact that the U.S. government is now being exponentially out-paced in research & development spending by the commercial sector, our greatest shortfall is not monetary. Rather, it is one of leadership.

As Capt. Eric Zastoupil, Conqueror 6, commander of C Company, 781 MI Battalion, notes, to regain our competitive advantage "there must be a shift in the way we allow ideas to grow and how we approach problems."

To do this, leaders must value trust and empowerment.

We must adopt the mindset that "failing fast and failing cheap" is always preferable to "failing expensively in the long-run".

- To do this, leaders must be "opportunity-focused instead of risk-focused".
- We must not buy yesterday's technology to solve tomorrow's problems.
- To avoid this predicament, leaders must drive a sense of urgency.

If leaders overcome all three of these shortfalls, we will foster a culture of adaptability, agility, and cohesion across the enterprise – our toughest and most important challenge of all. As Capt. Iain Cruickshank, Legion 6, former Delta company commander, asserts, "the Army Cyber Enterprise is not a reality but rather a goal to aspire to… [so] we should seize every opportunity to gain war fighting experience in cyberspace and adjust our organizations and systems based on the battles." With experience conducting our wartime mission, we will build the enterprise culture we need - an interdependent Team of Teams – an Army Cyber Enterprise.

"Vanguard! When Others Cannot!!"

Intern Program Prepares Officers for Cyber Battlefield

By Steven Stover, public affairs officer, 780th Military Intelligence Brigade

FORT GEORGE G. MEADE, Maryland – Capt. Joseph Casey (left), 781st Military Intelligence (MI) Battalion, receives his graduation certificate from Col. Dave Branch, commander of the 780th MI Brigade, after completing the Intelligence and Security Command, Army Intelligence Development Program – Cyber course, in a ceremony at the National Security Agency Cryptologic Museum on June 23.(U.S. Army Photo)

Capt. Joseph Casey, 781st Military Intelligence (MI) Battalion, 780th MI Brigade, was an Army of One when he graduated from the Intelligence and Security Command (INSCOM) Army Intelligence Development Program – Cyber, in a ceremony at the National Cryptologic Museum here on June 23.

AIDP-C is managed by the MI Branch at the U.S. Army Human Resources Command and is intended to prepare officers to serve in positions requiring cyberspace operations expertise.

According to Maj. Rachael O'Connell, the 781st MI Battalion's operations officer and AIDP-C program manager, those selected for the internship travel to Fort Meade for a two-year tour that consists of separate six to eight month operational assignments in up to four work centers at the National Security Agency (NSA) and U.S. Cyber Command (CYBERCOM). Additionally, the program includes formal instruction at the National Cryptologic School, Department of Defense cyber-related courses, and commercial training opportunities such as Network +, Security +, and Certified Ethical Hacker certifications to enhance the student's cyber skills.

"Coming into the program, I didn't have a lot of cyber background," said Casey. "Now, I feel confident that I could go into any cyber or intelligence role and bring this skill set to the fight."

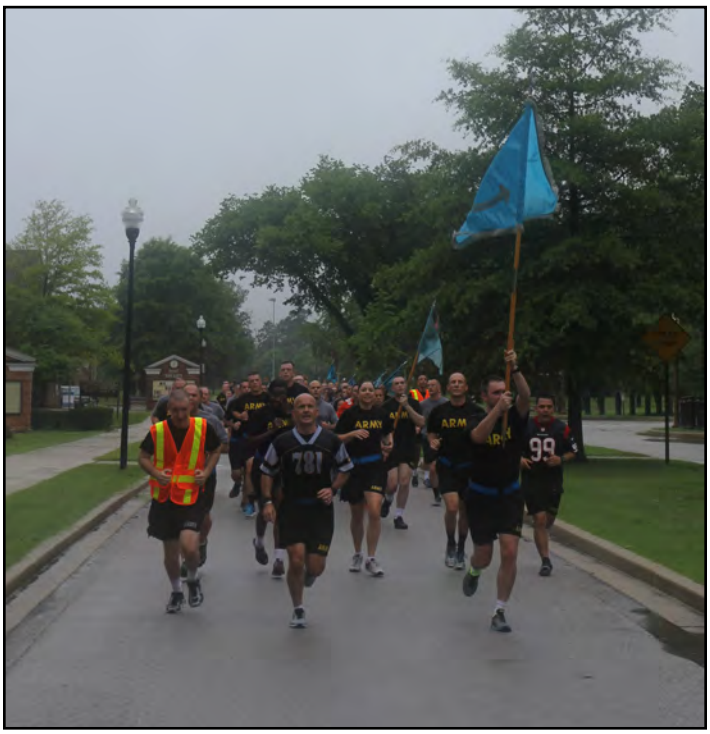
Col. Dave Branch, the presiding officer for the ceremony and commander of the 780th MI Brigade said Casey made significant contributions to the brigade and our partners during the program.

"Joe had the opportunity to work hand in hand with partner agencies such as the New York FBI field office Cyber Division," said Branch. "In the face of today's cyber threats, the relationships we build are essential to enable us to share knowledge across the intelligence community in order to stay ahead of our adversary. Joe, I challenge you to continue to foster those relationships."

Branch said that Casey also served operational tours with the NSA and with CYBERCOM's Cyber National Mission Force.

"Particularly as we see the battlefield environment changing," said Casey. "It is important that we have officers that understand the cyber environment and are able to leverage our technologies and our capabilities against the adversary."

Military Intelligence officers can apply for the nominative AIDP-C two-year internship through the MI Branch which typically selects two participants per year.



FORT GEORGE G. MEADE, Maryland – Soldiers from the 781st Military Intelligence Battalion (Cyber), Vanguard, participated in a four-mile battalion run to solidify their camaraderie and esprit de corps on July 7. (U.S. Army Photo)

Army Establishes Cyber Solutions Development Capability

By Steven Stover, public affairs officer, 780th Military Intelligence Brigade

FORT GEORGE G. MEADE, Maryland – The Soldiers of the Cyber Solutions Development Detachment will enable operational effects in and through the cyberspace domain by delivering timely, integrated, and innovative solutions that enable freedom of action required to support Army and Joint Force requirements, while denying the same to our adversaries. (U.S. Army Photo)

FORT GEORGE G. MEADE, Maryland - A new chapter was started for the Army presence in cyberspace when the 780th Military Intelligence (MI) Brigade officially organized a provisional Cyber Solutions Development (CSD) detachment under the 781st MI Battalion at Club Meade on July 25.

In a ceremony steeped in military tradition, the detachment's guidon was uncased for the first time and Maj. Todd Arnold, the officer who led the effort to make this vision a reality, passed the guidon to the incoming officer in charge, Maj. W. Michael Petullo.

According to Arnold the CSD detachment was formed to consolidate previously-dispersed cyberspace tool developers, and focus efforts to build solutions for both the DoD's Cyber Mission Force (CMF), and Army-specific cyberspace needs.

"The Army has requirements – beyond just the Cyber Mission Forces – to create capabilities. Before the CSD, there was no specific unit for that. The CSD is now filling that gap," said Arnold.

Before the CSD, a new capability request from a CMF team was often limited in responsibility to developers assigned to that single team. The launch of the CSD brings together a dedicated group of experts who can share knowledge, collaborate on solutions, and more rapidly deliver advanced cyberspace tools to the Army and multiple CMF teams. The CSD will draw upon more of the dynamic, rapidly-evolving cyberspace environment than any one team could, and better deliver capabilities for Army forces to counter adversary actions in cyberspace.

"There was a realization that it is important to have a cadre of technical engineers, software developers, in uniform, to produce solutions that will be applied in cyberspace, whether they be the equivalent to a weapon system or studying the defensive side of our posture," said Petullo. "We are the Army's organization that produces technical advancements to strengthen our force in cyberspace or use them in defense against adversaries."

Though the ceremony marked the official establishment of the CSD detachment, the unit is already having a positive impact on Army and Joint forces. The CSD supports contingency operations, Cyber Electromagnetic Activities Support to Corps and Below, and Army efforts to secure weapons and vehicle platforms against cyber vulnerabilities.

The CSD detachment will also support one of the three fundamental priorities for U.S. Army Cyber Command: to "design, build, and deliver integrated capabilities for the future fight".

"The CSD is something that we've thought about for a long time," said Lt. Gen. Paul Nakasone, the commanding general of U.S. Army Cyber Command. "Today is an important day for us because we were able to take an organization and put together our developers, who are critical to our future success... These are the folks that are going to build our capabilities for the future. Not only the close fight, but in the long term as we take a look at the threats to our nation."

Cyber Civilian Deploys in Support of the Warfighter

By Pedro Santiago Gonzalez, deputy team lead, 44 National Mission Team, C Company, 781st MI Battalion

ERBIL, Iraq – The author, with the rest of the team while supporting US Cyber Command and the Cyber National Mission Force during Operation Inherent Resolve. (Personal Photo)

My name is Pedro Santiago-Gonzalez, currently the Deputy Team Lead for 44NMT. I have been in or around Cyber/Intelligence since 2002 when I joined the Navy. I recently deployed on behalf of U.S. Cyber Command (USCYBERCOM), Cyber National Mission Force (CNMF), and the 781st Military Intelligence (MI) BN to Iraq.

The Command was looking for a senior member of CNMF to go and represent the organization with Combined Joint Task Force Operation Inherent Resolve. Since this would be the first deployment of a cyber planner from USCYBERCOM in support of this particular Joint Special Operations Command (JSOC) task force, I decided to volunteer for the position. I felt obligated to support the war fighter in any way that I could. I was fortunate enough to be selected by U.S. Army Cyber Command to not only represent the CNMF, but USCYBERCOM and the 781st.

I didn't deploy alone; however, there were early challenges due to the accelerated timeline of the deployment. Most of the challenges fell in the Civilian Personnel Office (CPO) area. This being the first time a battalion civilian member deployed, a rapid, repeatable process for deployment was undefined. There were plenty of items that needed to be checked off the deployment checklist in order for me to have a successful deployment. Most of the items were pay entitlements, which were rectified once CPO researched the processes. To complicate matters, it was a challenge for me to keep in communications with battalion CPO while deployed. For those of us who did not have an unclassified computer, there was only one common unclassified laptop for the entire Joint Operations Cell (JOC) to use. This made it difficult for me to receive, sign, and scan the necessary documents that CPO needed to rectify the issues. With determination and support from the deployed unit, I was able to get all necessary documentation to the battalion CPO for processing. These difficulties with pay processing were the only challenge that I encountered throughout the deployment period -- and after. Otherwise, everything went smoothly in regards to travel, getting to Iraq and returning.

The deployment experience was new to me. I am prior service Navy, so I have never deployed downrange before. I was looking forward to it – I was excited!

I had heard many stories from different people on what to bring and what to expect. I took their advice and packed all of the essentials that the previous commander of C Company, 781st MI Battalion, Capt. Lucas Holmbeck and the current commander of A Company, 781st, Capt. Hunter Hutcheson advised me to take. Those essentials came in handy and I do not know what I would have done if I did not pack them.

I arrived and they placed me into the Signal Intelligence (SIGINT) cell, doing analysis. I have been doing SIGINT analysis for over 10 years, so I quickly felt comfortable in that domain. I quickly realized that the analysts working there were all junior, and did not have a structured way of tracking their work and analytic results. When I arrived, I helped them create an internal request for information (RFI) tracker, and

Continued on page 35

Cyber Soldiers offer capabilities to tactical

By Steven Stover, public affairs officer, 780th Military Intelligence Brigade

FORT IRWIN, California – Army Chief of Staff Gen. Mark A. Milley listens to a briefing from Soldiers of the 780th Military Intelligence Brigade during a visit to the National Training Center at Fort Irwin, Calif., May 9, 2017. The Soldiers, members of the brigade's Cyber Electromagnetic Activities (CEMA) Support to Corps and Below (CSCB) Team, are conducting CEMA in support of a training rotation by the 2nd Armored Brigade Combat Team, 1st Infantry Division, as part of the Army Cyber Command-led CSCB initiative to help the Army define expeditionary cyber capabilities and their integration into maneuver unit planning processes. ((U.S. Army Photo)

The term "cyber Soldier" sounds like something out of a futuristic action film. But that's exactly what to call the Soldiers from the 780th Military Intelligence (MI) Brigade who serve under U.S. Army Cyber Command (ARCYBER). These Soldiers are part of the elite team at ARCYBER tasked with defending Army networks and providing full-spectrum cyber capabilities.

In addition, the 780th MI Brigade also conducts expeditionary cyberspace operations and training in support of armored brigade combat teams stationed at the National Training Center, Fort Irwin, Calif. It has offered home station training for the 2nd Armored Brigade Combat Team, 1st Infantry Division (2-1 ABCT), Fort Riley, Kan., in preparation for their NTC rotation since last November.

This is not the first time the cyber brigade has supported an Army combat training center rotation. ARCYBER established a pilot program in 2015 to build unit cyber capacity and to help the Army to operationalize cyber at all echelons. Additionally, the program seeks to strengthen other capabilities including information operations, intelligence and electronic warfare.

Helping tactical units maintain the initiative in cyberspace requires clear communication between the cyber brigade and the tactical unit's leaders. "From our experience over several rotations, we have learned that early integration with the supporting BCT is paramount to success at NTC," said Lt.

FORT IRWIN, California – Soldiers of the 780th Military Intelligence Brigade's Cyber Electromagnetic Activities (CEMA) Support to Corps and Below (CSCB) team conducts cyberspace operations in support of a training rotation by the 2nd Armored Brigade Combat Team, 1st Infantry Division, at the National Training Center at Fort Irwin, Calif., in May 2017. (U.S. Army Photo)

units

FORT IRWIN, California – Pictured are Soldiers of the 781st Military Intelligence Battalion's Cyber Electromagnetic Activities (CEMA) Support to Corps and Below (CSCB) team at the National Training Center, Fort Irwin, Calif., May 2017. (U.S. Army Photo)

Col. Justin Considine, commander of the 781st MI Battalion, Fort Meade, Md.

"Only when we gain the trust and confidence of the BCT Commander and his staff are we able to successfully integrate our capabilities into his operational planning," he said. "Simply put, the supported Commander will not trust our technology if he does not trust that we are members of his team. This process begins at the BCT's home station six months prior to NTC and also ensures our [cyber] troops understand as much as possible about how the BCT fights and what is important to the Commander."

Additionally, the 780th MI Brigade has also trained units to develop cyber warfighting scenarios that enhance the cyber training environment at NTC. According to Maj. Scott Bobier, the 781st MI Battalion executive officer, "This program offers maneuver combat units awareness of cyber key terrain that, if controlled, will provide a clear tactical advantage."

The training also offers feedback for the cyber brigade as well, helping to inform Army discussions about offensive and defensive cyber doctrine that will help define the future structure and integration of cyber training and support into tactical units and decision-making processes.

What we are learning and applying must be applicable to real-world operations, which is the ultimate test of anything conducted in a training environment," said Considine. "Secondly, the future of multi-domain battle demands we build our capacity to conduct expeditionary cyber warfare in all phases of operational planning -- from initial access and reconnaissance in Phases 0 and 1 through open hostilities in Phase 2 and 3."

FORT IRWIN, California – Spc. Rodolfo Lara, a member of the CEMA team, 781st Military Intelligence Battalion, conducts cyberspace operations in support of a training rotation by the 2nd Armored Brigade Combat Team, 1st Infantry Division, at the National Training Center at Fort Irwin, Calif., in May 2017. (U.S. Army Photo)

FORT GORDON, Ga. – Lt. Col. Dave Chang, the outgoing commander of the 782nd Military Intelligence (MI) Battalion, signified he has relinquished his command when he passed the battalion colors to Col. Dave Branch, commander of the 780th MI Brigade, on Barton Field Parade Grounds, June 2. (U.S. Army Photo)

Cyber Legion, a

By Steven Stover, public affairs office

FORT GORDON, Ga. – The outgoing commander of the 782nd Military Intelligence (MI) Battalion, Lt. Col. David Chang, talks about his past two years of command as a "tale of two quotes."

Chang's first brigade commander, Col. Joe Hartman, told him "…get all of your teams to FOC (Full Operational Capacity), on time, or you're fired," and his current commander, after receiving in-briefs about the organization a year ago, summed up his thoughts in three letters, "Wow."

Chang relinquished his battalion command to Lt. Col. Matthew Lennox, in a ceremony presided over by Col. Dave Branch, commander of the 780th MI Brigade, and Command Sgt. Maj. Sheldon Chandler, the brigade's senior enlisted leader, on Barton Field Parade Grounds, June 2.

Chang, who has been with the Cyber Branch since its inception in September 2014, has served with the same organization since 2008 – initially, with the U.S. Army Network Warfare Battalion, which became the 744th Military Intelligence Battalion, the precursor to the 780th MI Brigade, and finally as the 782nd MI Battalion commander. He leaves command, deflecting praise to his Soldiers, Civilians and the Families that supported them. He departs, leaving behind a legacy of firsts – firsts in the Army and firsts in the Services.

"The 782nd is the first command in any of the Services across the United States Cyber Command to bring all teams to fully operational capacity," said Branch. "This means that 782nd has 14 cyber teams across Georgia, Maryland, Texas and Hawaii that are prepared to count-

"Tale of Two Quotes"

er, 780th Military Intelligence Brigade

er our adversaries in cyberspace."

The unit also established a co-located operations and capabilities development element. "This combined force is quickly becoming the recognized model for how best to execute rapid, agile cyberspace operations," said Branch. "These efforts are informing our Army leaders and Sister Services of what is truly possible in the cyberspace domain."

Branch went on to say the battalion conducted synchronized cyber operations in support of the warfighter mission on the battlefield, earning the unit a reputation of success. He said that some of these operations cannot be discussed publicly due to their classification.

The new battalion commander for 782nd, Lt. Col. Lennox, is very well known in the cyber community. Lennox was an aide to the Commander of US Cyber Command / Director of the National Security Agency and was in charge of a National Mission Team. In his previous assignment, he was the deputy operations officer (J3), Army's Joint Force Headquarters-Cyber.

"As I've been watching from the Joint Force Headquarters, the 782nd continues to grow and mature in operational effectiveness," said Lennox. "This young battalion has already made a great name for itself and made important contributions to the [forward] forces. I'm truly honored to join the team today."

FORT GORDON, Ga. – Lt. Col. Matt Lennox, commander of the 782nd Military Intelligence (MI) Battalion, officially assumed command when he accepted the battalion colors from Col. Dave Branch, commander of the 780th MI Brigade, on Barton Field Parade Grounds, June 2. (U.S. Army Photo)

Chang is heading off to the Senior Service College, the Dwight D. Eisenhower School for National Security and Resource Strategy, Fort McNair, Washington, D.C., in July.

Joint Force Integrations and Partnerships

By Maj. Marlon Mallory, commander, Detachment Hawaii, 782nd Military Intelligence Battalion

Detachment Hawaii and its two teams are in a unique position, operationally and geographical. Aside from the tropical paradise that is Hawaii, more important is the access and partnership with local Army commands, sister services, and a Geographical Combatant Command (GCC), in this case, U.S. Pacific Command (USPACOM). Additionally, each service maintains units and headquarters from tactical to operational, all within a 30-mile radius. Exposure to these unique organizations provides the detachment with an exceptional large sphere of influence for the largest Combatant Command (COCOM) in the U.S. Military.

U.S. Pacific Command

Detachment Hawaii teams routinely provide cyber operational planning support to USPACOM during high-level command and control exercises. Partnering with USPACOM exposes our Soldiers to Joint Operations Planning Process (JOPPS), multinational and interagency partnerships, and transition from operational plans to an execution order. The knowledge and skill quickly feed COCOM planners with a level of tactical understanding never seen before. Both the teams and COCOM planners share the lesson learned, develop Tactics, Techniques and Procedures (TTPs) and develop their understanding of delivering effects and through cyber.

Multiservice Partnership

The team assigned to DET-HI are a unique to take advantage of the Services in the area. The teams have significantly befitted partnership with the 613th Air Operation Center (AOC). The AOC serves as the nerve center of air operations during any campaign within the PACOM AOR. The team's partnership with the AOC provides increased understanding on kinetic and non-kinetic effects synchronization and lines of effort that further provide the widest range of options available to the combatant commander or a Joint Force commander.

Another unique advantage the teams have is our ability to leverage subject matters expertise across the services. Other service teams aligned to USPACOM bring a wealth of experience and understanding when analyzing near-peer threats and their more conventional forces. Similarly, Detachment-Hawaii provides planning expertise, an attribute to the Army's effort to train all leaders on the operations process through Troop Leading Procedures and or the Military Decision Making Process (MDMP). The Operational Headquarters (OPCON) and adjacent teams routinely seek out our Officers, Warrant Officers, and NCOs for their abilities to intelligence, planning, and operations.

U.S. Army Pacific

U.S. Army Pacific (USARPAC) is a unique Army Command and itself based their geographical location, wide range of tasks and mission complexity. The USARPAC Commander, Gen. Robert Brown, recognizes the level of effort required to meet these challenge and directed his staff to leverage any and all capabilities available and set conditions for mission success. In doing so, USARPAC routinely reaches out and relies on Detachment Hawaii to provide knowledge and understanding on cyber operations, PACOM aligned Cyber Mission Forces, and Target Development to list few. Partnership with USARPAC provides our teams with access to mission-enabling capabilities, and the respect of the largest Army Service Component Command.

Detachment Hawaii's collaboration with USARPAC also provides our Soldiers and leaders with a unique opportunity to contribute and influence Multi-Domain Battle (MDB) development. U.S. Army TRADOC defines the Multi-Domain Battle as "an emerging concept between the Army and Marine Corps, in concert with the Joint Force, to help maintain American military dominance in all five domains." Recently, USARPAC, was identified as the lead for

Continued on Page 36

131As in the Cyberspace Domain

By Chief Warrant Officer 3 Harry Burgess, Fires Planner, Detachment Texas, 782nd Military Intelligence Battalion

The Field Artillery Targeting Technician (131A), provides targeting expertise in all war fighting domains ensuring Warfighters can maintain an advantage over our adversaries. The 131A Corps has transitioned from maintenance and repair of Fire Finder RADAR systems to running the Army Targeting process at multiple echelons and supporting the Joint Targeting process. They are responsible for maintaining the Army's Target Mensuration Only (TMO) program for employment of precision munitions and have begun to reenergize the Systems Integrator role, which provides expertise when integrating multiple fire control and fires planning systems.

Along with these new initiatives, 131As now integrate effects conducted in Cyberspace as a Fires Planner/Targeteer. Each of these roles could conceivably be their own MOS, yet mastering each of these roles will make a senior 131A a true subject matter expert (SME) in our field; understanding how and when to leverage capabilities to identify threats in the area of operations, while ensuring the ability of communication between command systems in order to apply targeting processes so as to provide the appropriate response to identified targets that will meet the commander's intent.

Senior 131As at U.S. Army Cyber Command (ARCYBER), such as Chief Warrant Officer 4 Tom O'Neill, have done a remarkable job in building out positions for 131As in this domain, but the question of how do we move forward is beginning to arise. An early 131A pioneer into cyber, Chief Warrant Officer 3 Jordan Kness, is headed to Fort Sill, Oklahoma, to begin his next assignment as an instructor for the 131A Basic Course; the intent is to share knowledge of previous assignments, to include cyber, with the newest 131As. For the rest of the 131As in cyber, the question still remains, what do we do after our cyber tour?

O'Neill has worked diligently with the 131A Branch manager to allow us follow on assignments under Combatant Commands (COCOM) we have supported so we can carry on with the missions we have been working, unfortunately Permanent Change of Station (PCS) windows and open positions at those units does not always align. The Army is currently building 131A positions at the Joint Force Headquarters (JFHQ) Forward, this only effects those elements aligned to ARCYBER. While those of us PCS'ing from our positions in cyber will be able to assist any unit we get assigned to further their understanding of Cyberspace capabilities and planning, the ability to step in with the knowledge of planning efforts already being conducted by the units we have been supporting will allow us to move forward more rapidly if we PCS to those units we have already been supporting.

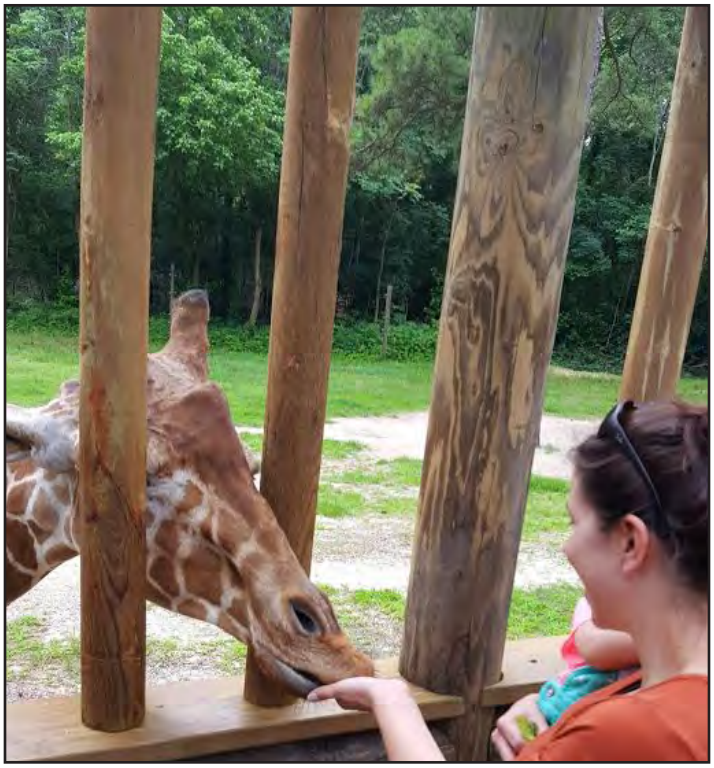
In U.S. Army Forces Command (FORSCOM), 131A's typically serve their junior time (Warrant Officer to Chief Warrant Officer 2) at the battalion-level, serving as a Target Acquisition Platoon Leader (TAPL) or a battalion targeting officer. After successful battalion assignments, 131As will move to BDE (Chief Warrant Officer 2 and 3) or division positions (Chief Warrant Officer 2 to 4) and use their experience to plan at those echelons while mentoring junior 131A's at the lower echelons. The debate then begins on when and where should a 131A be positioned to allow the best professional growth opportunities with a well- rounded understanding of all domains; although 131As need experience in FORSCOM before entering Cyber. Should Cyberspace positions mimic FORSCOM and have a Chief Warrant Officer 2 or 3 at the Cyber mission Team and National Mission Team level (CMT/NMT), Chief Warrant Officer 3 and 4 at the JFHQ (which there is currently not a position), Chief Warrant Officer 4 and 5 at ARCYBER and U.S. Cyber Command level? Another major concern, echoed by Chief Warrant Officer 5 Robert Wilson (Field Artillery Chief Warrant Officer of the Branch) during his May visit to National Security Agency-Texas, is that 131As need to be

Continued on page 36

Centurions Take Over Riverbanks Zoo

By Capt. Brian Ellis, 782nd Military Intelligence Battalion (Cyber)

COLUMBIA, South Carolina – In early June, Charlie Company, 782nd Military Intelligence Battalion, took a break from their busy work schedules to come together, build morale, and foster relationships amongst the unit at the Riverbanks Zoo in Columbia, South Carolina. The Family Readiness Group (FRG) comprised of Soldiers and their Families gathered at the zoo and then came together for lunch at Fuddruckers afterwards for burgers, milk shakes, and giant rice crispy treats.



The company embodies a philosophy of achieving the appropriate balance between duty and family. Centurion Soldiers earned a few hours to relax, foster relationships and spend quality time with their Families prior to executing a two and a half weeks' Mission Readiness Exercise. The Company FRG and Staff Sgt. Bethany Collins diligently planned and resourced multiple fundraisers over the past several months to enable over 70 Soldiers and their Families to attend at no cost. The Riverbanks Zoo was the perfect venue for single Soldiers and Army Families to engage in ropes courses, feed giraffes by hand, and celebrate the end of the school year.

Army Trains Soldiers as Cyberspace Solution Engineers

By Steven Stover, public affairs officer, 780th Military Intelligence Brigade

FORT GEORGE G. MEADE, Maryland – The 2017 Tool Developer Qualification Course graduates: Spc. Matthew Alderman, C Company (Co.), 781st Military Intelligence (MI) Battalion (Bn.); Sgt. Daniel Cardinale, B Co., 781st MI Bn.; Spc. Stephen Ciullo, E Co., 782nd MI Bn.; Spc. Alexander Dow, A Co., 782nd MI Bn.; Spc. Daniel Ems III, C Co., 742nd MI Bn., 704th MI Brigade; Spc. Andrew Fricke, A Co., 781st MI Bn.; Spc. Tyler Gantt, C Co., 781st MI Bn.; Sgt. Jonathan Haubrich, A Co., 782nd MI Bn.; Spc. Steven McMaster, C Co., 782nd MI Bn.; Staff Sgt. Saurabh Roy-Chowdhury, B Co., 781st MI Bn.; Spc. Jeremy Ryan, C Co., 782nd MI Bn.; Sgt. Jesse Schoenwald-Oberbeck, A Co., 781st MI Bn.; Spc. Steven Solis, A Co., 782nd MI Bn.; Sgt. Brian Stout, E Co., 782nd MI Bn.; Spc. Sean Stuessel, B Co., 782nd MI Bn.; Spc. Marlin Washington, A Co., 781st MI Bn.; and Sgt. Eunho Yeo, HHC, 781st MI Bn. (U.S. Army Photo)

FORT GEORGE G. MEADE, Maryland – The 780th Military Intelligence (MI) Brigade partnered with the University of Maryland Baltimore County (UMBC) Training Center to build the course curriculum and provide instruction for the Tool Developer Qualification Course (TDQC) and on July 28 the second graduating class received their certificates of completion at the Fort Meade Post Theater.

TDQC is an intense 35-week education program designed to educate individuals who have little to no computer programming experience and have been identified through an assessment as having the aptitude and desire to become a computer programmer.

"The course helped deepen the concepts and reinforce those things I did know – It was a confidence booster," said Spc. Marlin Washington, 781st MI Battalion, the distinguished honor graduate for the class. "The biggest takeaway was how it (taught me how) to research."

According to the TDQC program manager, Chief Warrant Officer 4 Thomas Bichard, graduates of the TDQC are proficient to an intermediate level in creating programs using the C and Python computer programming languages. The TDQC provides an education path for individuals to become experienced at approximately 90 percent of the identified critical developer requirements that an individual must be able to articulate and demonstrate through practical application in order to be certified as a Cyberspace Solution Engineer.

A Cyberspace Solution Engineer is a versatile, highly trained individual responsible for the analysis of system vulnerabilities, product research, cyberspace solution development, documentation, and implementation of software and hardware solutions that operate in and through cyberspace and serve as a force multiplier for maneuver forces.

"The course teaches the basic concepts of programming and quickly gets you to a level where you can be beneficial to a (cyber) team producing useful programs," said Spc. Andrew Fricke, 781st MI Battalion, the honor graduate for the class.

Chief Warrant Officer 5 Mark Mollenkopf, the command chief warrant officer for U.S. Army Cyber Command (ARCYBER) was the guest speaker at the ceremony and challenged the graduates with humor in his remarks.

"Cultivate passion for what you do and for those around you," said Mollenkopf. "It's wise to avoid going too far (into debates) that often crop up such as VI versus EMACS, Python versus PhP, Tabs versus White Space, Java versus .Net. These can be humorous diversions, but if taken too far can negatively affect the team culture and create an unproductive cliquish work environment."

To date, there have been 29 graduates from the course. The third iteration of the course is currently in session at Fort Gordon, Georgia, and the fourth iteration is scheduled to start at the UMBC Training Center in September.

Army Cyber Guard Transition Ceremony Historic

By: Steven Stover, public affairs officer, 780th Military Intelligence Brigade (Cyber)

Col. Adam Volant, the Task Force Echo commander, stands in formation with his Soldiers during a transition of authority ceremony here, Aug. 15. (U.S. Army Photo)

FORT GEORGE G. MEADE, Maryland -- The transition of authority between 169 Cyber Protection Team (CPT) and Task Force Echo (TFE), U.S. Army National Guard (ARNG), at the McGill Training Center August 15 was more than just a ceremony -- it was a historic and impactful event for the Army cyber enterprise and the Nation.

While Active Duty, U.S. Army Reserve and ARNG units frequently train, deploy, and serve side-by-side -- the event marked the first ARNG task force mobilization of this size to support U.S. Cyber Command (USCYBERCOM) operations full time, and is a testament to the Army's commitment to the Total Force in defense of networks against the Nation's adversaries.

Lt. Gen. Paul Nakasone, commander of U.S. Army Cyber Command (ARCYBER), hosted the event, which included honored guests Governor of the Commonwealth of Virginia Terry McAuliffe, Lt. Gen. Timothy Kadavy, director of the Army National Guard, as well as numerous State Adjutants General, other distinguished guests, Soldiers, and their Family members.

In his remarks, Nakasone talked about an Army that has been at war for 16 years, the longest period in our Nation's history, and how the Army recognizes the future is fraught with many challenges, but also with many opportunities.

"Our Total Force Army -- our Army National Guard, our Army Reserve, all of these Soldiers, including the active component, will play a significant role in the future of securing cyberspace defense for our Nation," said Nakasone. "169 Cyber Protection Team has set the stage for the future. They have literally brokered for our Nation a future cyberspace operations capability."

169 CPT has been operating under the 780th Military Intelligence (MI) Brigade (Cyber), an active component organization, since 2015. Presently, 169 CPT and its 21 ARNG Soldiers hail from 13 States. At the unit's largest formation, more than 60 Soldiers were assigned to 169 CPT, representing 24 States and two U.S. territories.

According to Lt. Col. Martine Whitaker, chief of 169 CPT, the team is the first ARNG cyber team to reach Initial Operating Capability (IOC), and did so in stride with their active duty counterparts. More importantly, the team leaves Fort Meade with the cy-

Lt. Gen. Paul Nakasone, commanding general of U.S. Army Cyber Command, presides at a transfer of authority ceremony between the Army National Guard's Task Force Echo and 169 Cyber Protection Team, , at the McGill Training Center here, Aug. 15. (U.S. Army Photo)

Moment

Lt. Gen. Timothy Kadavy, director of the Army National Guard, speaks at a transfer of authority ceremony between the Guard's Task Force Echo and 169 Cyber Protection Team, at the McGill Training Center here, August 15. The general discussed the importance of the National Guard cyber force to the Total Army, the Department of Defense and the Nation. (U.S. Army Photo)

berspace operational knowledge, skills, and abilities, which will benefit their home states, the Army, and ultimately, the Nation.

"Today, we proudly recognize the National Guard's absolute, indisputable relevance within the Total Army," said Whitaker. "In the case of 169 CPT -- the first ARNG cyber team to serve alongside our active-duty comrades -- 169 will always be the first, the original, the mold from which all other teams follow."

"The performance of 169 CPT and assumption of mission by Task Force Echo demonstrates the Total Force employed in the Army and USCYBERCOM," said Col. Adam Volant, the TFE commander.

"Together, we integrate with ARCYBER and USCYBERCOM to perform missions that defend the Nation and represent the quality force effectively aimed against our adversaries."

According to Volant, both TFE and 169 CPT Soldiers have strong academic, interagency and corporate relationships.

"The truly unique part of these Soldiers is that the blend of their experience, military training and civilian credentialing -- cybersecurity certifications and clearance -- make them well qualified to immediately perform missions of importance at the State and Federal level," said Volant.

Of note, the ARNG recently established a mission-ready cyber unit -- the 91st Cyber Brigade, which is comprised of five cyber battalions. 169 CPT moves to a new chapter under the Maryland ARNG and will assist the 91st Cyber Brigade with the readiness of future teams.

"Today is truly a great day," said Kadavy. "Not just for the Total Army and the Department of Defense, but for our entire country, as Task Force Echo assumes the mission from the 169th Cyber Protection Team…they represent the precursor to the reserve mission-ready cyber units of today and the future."

As an integral part of the Army cyber team -- TFE and 169 CPT live up to the National Guard motto: "Always Ready, Always There!"

TFE replaces 169 CPT and is comprised of more than 140 ARNG cyber Soldiers representing seven states -- California, Georgia, Indiana, Michigan, Ohio, Utah, and Virginia. TFE will also operate under the 780th MI Brigade to train and conduct cyberspace operations in support of USCYBERCOM and the Cyber Mission Force.

Army National Guard Soldiers of the 169 Cyber Protection Team and Task Force Echo participate in a transition of authority ceremony at the McGill Training Center here, Aug. 15. (U.S. Army Photo)

More

TF Echo Aligns Under the 780th MI Brigade

By Steven Stover, public affairs officer, 780th Military Intelligence Brigade

FORT GEORGE G. MEADE Maryland – Col. Dave Branch, commander of the 780th Military Intelligence (MI) Brigade, and Command Sgt. Maj. Sheldon Chandler, the brigade's senior enlisted leader, watch as the cyber Soldiers of Task Force Echo, Army National Guard, change out their patches from their individual states to the patch of the 780th MI Brigade, during a patching ceremony here, May 25. (U.S. Army Photo)

FORT GEORGE G. MEADE, Maryland – Military cyber history was made when Task Force (TF) Echo, U.S. Army National Guard (ARNG) realigned under the 780th Military Intelligence (MI) Brigade in a Patching Ceremony at the Post Theater here, May 25.

The unit is comprised of ARNG Soldiers from California, Georgia, Indiana, Michigan, Ohio, Utah and Virginia, and upon completion of their initial training the unit will become an integral part of the U.S. Army Cyber Command under the 780th MI Brigade.

Prior to the patching ceremony, Col. Dave Branch, commander of the 780th MI Brigade, addressed the TF Echo Soldiers for the first time and told them the brigade has been anxiously awaiting their arrival.

"We've been anxiously awaiting Col. (Adam) Volant and Task Force Echo to get here because we've been doing this internally, without really a lot of structure," said Branch. "…amp up the fact that we only began (offensive cyber) operations a year ago – it is continuous now."

Up until now, 169 Cyber Protection Team (CPT), ARNG, has been augmenting the brigade. For the past two years, 169 CPT has worked with Active Army units to train and conduct cyberspace operations.

Branch told the TF Echo Soldiers they too will soon have an opportunity to make an impact within the cyber domain.

"Operators are on keyboard executing – time now – operations against the adversary. That's what you're getting ready to be a part of," said Branch. "Early mornings, late nights, weekends, what you're predecessors have built, and what is being executed now by teams both here and Georgia, and eventually in Texas and Hawaii, against other adversaries. This is real. The domain is real."

Branch has a goal for the newly formed unit to achieve over the next 12 months. He wants other military forces to tell TF Echo's story.

"When someone else is telling your story, you've achieved success. That's the mark for success that I want for Task Force Echo," said Branch.

TF Echo Soldiers will eventually return to their home stations as members of a newly formed cyber unit and put on the patch of the 91st Cyber Brigade, ARNG.

"At the moment we took off our patches this morning something larger happened in the Army, in the Total Force, and certainly in the Army National Guard. When you return to your respective States, the likelihood of putting the patch that you took off this morning back on is not there," said Col. Adam Volant, commander of TF Echo. "Because during that time we were mobilized, notified of our opportunity to serve here with this command, the Army National Guard created a cyber brigade of which you are a great and stable part, the first part…the pioneers."

Army Recruiting Hosts Educator's Tour, Visits Cyber

By Steven Stover, public affairs officer, 780th Military Intelligence Brigade

Toni Pisciotta, right, an individual training specialist, and Tracy Manassa, left, a cyber planner, assigned to the 780th Military Intelligence Brigade operations (S-3) training and exercise section, talk to educators and Army recruiters about the brigade's cyber mission force training model as part of an educator's Science, Technology, Engineering, and Math tour, at the MI brigade headquarters here, May 3. (U.S. Army Photo)

FORT GEORGE G. MEADE, Maryland – Educators from the Southwestern United States and their escorts from the U.S. Army 5th Recruiting Brigade met with Soldiers and civilians with the 780th Military Intelligence (MI) Brigade to discuss education and training opportunities, and the mission of the cyberspace workforce at the MI brigade headquarters here, May 3.

The meeting engagement was one of several stops during an educator's Science, Technology, Engineering, and Math (E/STEM) tour in the D.C. area to showcase the Army's commitment to supporting today's educators and students.

The educators were interested in what training programs and opportunities the Army has to offer, but were equally interested in how their school districts could prepare their students for a career in cyberspace operations.

Maj. Todd Arnold, Cyber Solutions Development Detachment, 780th MI Brigade, told the educators and recruiters that the Service's continued investment in personal education and conference attendance is one of the reasons cyber Soldiers stay in the Army; however, it takes a special Soldier to make it through the rigorous training curriculum to become a cyberspace operations specialist, technician and officer.

"The Cyber branch does need Soldiers who are technically competent," said Todd. "However, we also need them to have the following characteristics: self-education and development, intellectual curiosity, inference, and critical thinking."

In addition to a discussion on the brigade's operations and the cyber mission force training model, the 780th MI Brigade had Soldiers of all ranks talk about their background, training, and what inspired them to be a cyber warrior. Because the cyber branch is only six years old, their individual stories were as informative to the Army recruiters and they were to the educators.

"I re-enlisted in the Army because it brought out something in me that I didn't see in myself; it gave me a confidence that I did not have before," said Spc. Kayla Lee. "I decided to stay as a 35N (Signals Intelligence Analyst) because I am passionate about what I do but I also get to watch the cyber field grow and evolve and I get to be a part of that. It will only get bigger and better from here."

According to Army Col. Terance Huston, the brigade commander of the 5th Recruiting Brigade, Fort Sam Houston, Texas, the E/STEM tour was part of a larger STEM campaign focused on highlighting the mainly intellectually rigorous and technologically cutting-edge career opportunities that the Army offers.

Soldiers assigned to the 780th Military Intelligence (MI) Brigade talk to educators and recruiters about their cyber training and education as part of an educator's Science, Technology, Engineering, and Math tour, at the MI brigade headquarters here, May 3. (U.S. Army Photo)

Army Cyber Command Honors Its Top Soldier &

By Steven Stover, public affairs officer, 780th Military Intelligence Brigade

FORT BELVOIR, Va. – Spc. Johnny Long of Mesquite, Texas, assigned to Detachment Hawaii, 782nd Military Intelligence (MI) Battalion, 780th MI Brigade, is shown here at the halfway point of a 12-mile road march on day three of the U.S. Army Cyber Command Best Warrior Competition near Pohick Neck, Virginia, August 23. (U.S. Army Photo)

FORT BELVOIR, Va. – U.S. Army Cyber Command named its best warriors of 2017 Aug. 25, after a week of intense competition here.

Spc. Johnny Long of Mesquite, Texas, assigned to Detachment Hawaii, 782nd Military Intelligence (MI) Battalion, 780th MI Brigade, Intelligence & Security Command (INSCOM), earned Best Warrior Soldier of the Year honors and Sgt. Kevin Beuse of Colorado Springs, Colo., assigned to Headquarters and Headquarters Company, 470th MI Brigade, INSCOM, was named Best Warrior NCO of the Year.

Soldiers from multiple commands actually started on the road to the ARCYBER title in early spring. It has been a grueling climb to the top with each Soldier tackling at least four other Best Warrior Competitions to reach the ARCYBER level. And there's still one more rung to go for Long and Beuse … representing ARCYBER at the Army-level competition in October.

Organizers of the ARCYBER event said the level of competition has never been higher, nor the physical and mental events more challenging. The Army's Soldier and NCO of the Year selection process became tougher following 9/11, when the Sergeant Major of the Army changed the process to more realistically prove the "Total Soldier" concept.

Long has a bachelor's degree in physics and joined the Army in 2013 after teaching high school because he wanted to serve. He is a Korean Linguist who aspires to join a SOT-A (Special Operations Team-Alpha), which is a signals intelligence–electronic warfare element of Army Special Forces. For Long, the BWC has been a series of opportunities, and he's had a lot of fun.

"I know that parts of it have been rougher than I expected, parts that were more fun than I expected. You never know exactly what to expect at each level," he said. "But there have also been a lot of opportunities for experiences that I wouldn't otherwise have had."

FORT BELVOIR, Va. – Command Sgt. Maj. William Bruns, command sergeant major of U.S. Army Cyber Command (ARCYBER), congratulates Spc. Johnny Long of Mesquite, Texas, assigned to Detachment Hawaii, 782nd Military Intelligence Battalion, after announcing his selection as the Best Warrior Soldier of the Year for ARCYBER at a ceremony in the command's headquarters, August 25. (U.S. Army Photo)

NCO for 2017

Long said those opportunities included hands-on experience with weapons that he hadn't handled since basic training; learning Army doctrine; and "definitely a lot of combat lifesaver practice." He's most looking forward to facing a selection board led by the Sergeant Major of the Army when he competes in the October event.

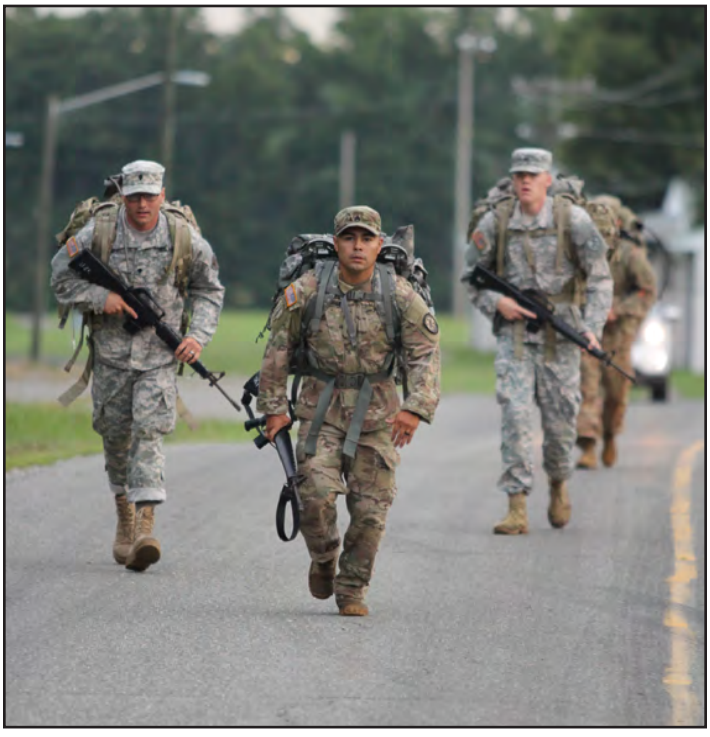
Beuse credits his mentor, Sgt. Stephen Pritchard, for getting him to this point in the competition. He also gave equal credit to his wife, who lives in Honduras, and who he says has always believed in him and knew he would win. Alongside his preparation for the competition, which began in February, Beuse has been working to bring his wife to the U.S.

At the ceremony naming the winners, Command Sgt. Maj. William Bruns, the ARCYBER command sergeant major, said he's very impressed with the calibre and character of this year's competitors.

"I think back to when I competed in boards, we were very knowledgeable,…but the knowledge of the Soldiers today is high…the bar is very high. The future of the NCO Corps is in good hands." said Bruns. "These Soldiers are really, really exceptional. I think we're going to do really well (at the next level of competition)."

FORT BELVOIR, Va. – Command Sgt. Maj. William Bruns, command sergeant major of U.S. Army Cyber Command (ARCYBER), congratulates Sgt. Kevin Beuse of Colorado Springs, Colo., assigned to Headquarters and Headquarters Company, 470th MI Brigade, after announcing his selection as the Best Warrior NCO of the Year for ARCYBER at a ceremony in the command's headquarters, August 25. (U.S. Army Photo)

FORT BELVOIR, Va. – Spc. Johnny Long of Mesquite, Texas, assigned to Detachment Hawaii, 782nd Military Intelligence (MI) Battalion, 780th MI Brigade, treats a simulated casualty after an ambush on day three of the U.S. Army Cyber Command Best Warrior Competition near Pohick Neck, Virginia, August 23. (U.S. Army Photo)



FORT A.P. HILL, Virginia – Staff Sgt. Humberto Gutierrez, Headquarters & Headquarters Company, 780th MI Brigade, is the Brigade's NCO of the Year, and after winning the North Region INSCOM event, he was selected as the runner-up at the INSCOM-Level (U.S. Army Photo)

ARMY VALUES

WWW.ARMY.MIL/VALUES

LOYALTY

Bear true faith and allegiance to the U.S. Constitution, the Army, your unit and other Soldiers. Bearing true faith and allegiance is a matter of believing in and devoting yourself to something or someone. A loyal Soldier is one who supports the leadership and stands up for fellow Soldiers. By wearing the uniform of the U.S. Army you are expressing your loyalty. And by doing your share, you show your loyalty to your unit.

DUTY

Fulfill your obligations. Doing your duty means more than carrying out your assigned tasks. Duty means being able to accomplish tasks as part of a team. The work of the U.S. Army is a complex combination of missions, tasks and responsibilities — all in constant motion. Our work entails building one assignment onto another. You fulfill your obligations as a part of your unit every time you resist the temptation to take "shortcuts" that might undermine the integrity of the final product.

RESPECT

Treat people as they should be treated. In the Soldier's Code, we pledge to "treat others with dignity and respect while expecting others to do the same." Respect is what allows us to appreciate the best in other people. Respect is trusting that all people have done their jobs and fulfilled their duty. And self-respect is a vital ingredient with the Army value of respect, which results from knowing you have put forth your best effort. The Army is one team and each of us has something to contribute.

SELFLE SERVICE

Put the welfare nation, the Arm subordinates be own. Selfless se larger than just In serving your you are doing y loyally without recognition or building block service is the co of each team m a little further, longer, and loo to see how he c to the effort.

ESS E

of the
ny and your
efore your
rvice is
one person.
country,
your duty
thought of
gain. The basic
of selfless
ommitment
ember to go
endure a little
k a little closer
r she can add

HONOR

Live up to Army values. The nation's highest military award is The Medal of Honor. This award goes to Soldiers who make honor a matter of daily living — Soldiers who develop the habit of being honorable, and solidify that habit with every value choice they make. Honor is a matter of carrying out, acting, and living the values of respect, duty, loyalty, selfless service, integrity and personal courage in everything you do.

INTEGRITY

Do what's right, legally and morally. Integrity is a quality you develop by adhering to moral principles. It requires that you do and say nothing that deceives others. As your integrity grows, so does the trust others place in you. The more choices you make based on integrity, the more this highly prized value will affect your relationships with family and friends, and, finally, the fundamental acceptance of yourself.

PERSONAL COURAGE

Face fear, danger or adversity (physical or moral). Personal courage has long been associated with our Army. With physical courage, it is a matter of enduring physical duress and at times risking personal safety. Facing moral fear or adversity may be a long, slow process of continuing forward on the right path, especially if taking those actions is not popular with others. You can build your personal courage by daily standing up for and acting upon the things that you know are honorable.

Cyber Soldier Makes Transition to Cavalry Scout

By: Steve Stover, public affairs officer, 780th Military Intelligence Brigade (Cyber)

Army Sgt. Brittany Wildman from Woodstock, Ohio, joined the Army to protect her Family and her country's way of life; however, she quickly learned that a desk job was not her style.

The former cyberspace operations specialist graduated from the Cavalry Scout, 19D military occupational specialty (MOS) M3 Bradley / Humvee course on July 30, and is heading off to the U.S. Army Airborne School in mid-August before going to her next duty assignment with the 82nd Airborne Division, Fort Bragg, North Carolina.

Goarmy.com, the Army's official recruiting website, states that cavalry scouts are the "eyes and ears of the commander during battle."

"When I was little it was always a dream of mine to be a Soldier," said Wildman. "As I grew up I learned my 'why'…and simply put it's my family. I could never imagine something bad happening to them or my home. I feel that it is my duty to protect them and my countries way of life from those who threaten it."

She credits her recruiter for her decision to join the Army. No one in her Family serves in the military – she's the first – however, the recruiter made her feel that the Army could be her extended Family and was where she belonged.

And while Wildman doesn't have any ill-feelings toward the Cyber branch, on the contrary she learned quite a bit, it just wasn't what she wanted to do.

"When I joined the Army, I wanted to be the boots on the ground, however, females were not allowed to be in these roles," said Wildman. "So, I went with this new MOS that I knew nothing about. I would quickly learn that a desk "computer" job was not my style."

She patiently waited for her retention window to open and immediately began pestering her unit Career Counselor about her options of switching to a more tactical field.

"Then one day the door opened up and I was able to chase my childhood dreams." Said Wildman.

Her role model and motivator throughout this process has been retired Lt. Col. Dan Schilling, a 30-year special operations and Black Hawk Down veteran. While he did not influence her decision to become a cavalry scout – he is someone she looks up to and she aspires to have the same experiences he had when he served in the military.

"In [Sgt.] Wildman I recognized the latent trifecta of adaptability, audaciousness and relentless pursuit of a goal. What she needed was encouragement and some direction," said Schilling. "From there, I knew she's self-actualized enough that those traits would land her in the right mission space with likeminded individuals. As indeed it appears to be doing. I'd predict the 82nd is merely a stop on the way to something blacker."

Wildman knows she's not the first female Soldier to transition to a Combat Arms branch, and that really wasn't her reason to make the move. It's simply something she has wanted to do since joining the Army and is thankful for the opportunity. She offers the following advice to others; regardless of their gender.

"For the last several years, I have been told by everyone that it will never happen, or I would never make it, and that it was unrealistic to want to join the combat arms, especially to leave cyber for that." said Wildman. "Despite being told by just about everyone to throw in the towel, I never gave up and here I am as a 19D."

And what are her career aspirations?

"My long term goal is to be the Sergeant Major of the Army."

Look out Sgt. Maj. of the Army Daniel Dailey, Wildman is gunning for your job.

FORT INDIANTOWN GAP, Pennsylvania – Sgt. Brittany Wildman sets a C4 explosive charge as part of her cavalry scout training in July. (Personal Photo)

780th MI Shuts Out 32nd IS in Division II Softball Final

By Tynise Jones, Fort George G. Meade Public Affairs Office

FORT GEORGE G. MEADE, Maryland – That's a big 25-0 "Donkey Smash" for the 780th MI's "Swamp Donkeys" moments after claiming the softball title Tuesday evening on Donahue Field. (Photo by Phil Grout)

After rain and lightning storms repeatedly canceled Fort Meade's intramural softball games, the 780th Military Intelligence Brigade and the 32nd Intelligence Squadron finally made it to the Division II championship round.

Under clear skies Tuesday evening on Donahue Field, the 780th's Swamp Donkeys shut out the 32nd's Blue Knights 25-0.

"This win was well overdue," Spc. Eric Robbins of the 780th said after the victory.

The 23-year-old resident of Freedom Barracks had a very simple strategy to win the game.

"I just stayed loose and ready," Robbins said.

Last week, the 780th defeated the 32nd, 21-6, in the first game of the three-game series. Both teams played in Tuesday's doubleheader to determine the champion.

The first game was tight. Both the 780th and the Blue Knights were neck-in-neck in the bottom of the third inning with a score of 4-4.

At the top of the fourth inning. the Blue Knights started to pull away, making it hard for the 780th to come back.

The Blue Knights won 12-9.

"We didn't really prepare ourselves for the first game," said Spc. Tyler Marden, head coach of the 780th.

However, the 780th redeemed themselves in the second game while hitting almost everything thrown their way.

By the end of the first inning, the team was up 12-0.

The 780th finished strong, defeating the Blue Knights 25-0 to gain the title.

"The second game was pretty cool," Marden said.

The 22-year-old was proud of the way his team came together to win the championship.

"We got off to a good start and played really good defense while leaving them scoreless," Marden said.

Spc. Brooke Mellors, head coach of the Blue Knights, showed good sportsmanship over the loss.

"We shut down mentally, but we didn't expect to make it this far," he said. "So it's still very exciting."

Beth Downs, sports specialist for the Directorate of Family and Morale, Welfare and Recreation, was happy with the games as well as the turnout.

"The games went very well," she said. "We had a nice crowd from not only family, but support from leadership as well."

At the end of the second game, both teams received trophies. The 780th was awarded a gold tournament trophy, while the Blue Knights were honored with a silver runner-up trophy.

The 780th also received championship beverage holders alongside their trophy created by the Arts & Crafts Center.

"I always said I wanted to play on a championship team, and now I'm here and it feels great," said Sgt. 1st Class Abraham Rodriguez of the 780th MI.

FORT GEORGE G. MEADE, Maryland – Blue Knights third baseman Airman 1st Class Jared Academia makes the out on 780th MI runner Staff Sgt. "Big Mac" Jacob McCormack who kicks up the dust on his belly slide. The 780th went on to win the Division II softball title. (Photo by Phil Grout)

Learning Enterprise

By: Capt. Shane Sartalamacchia, commander, Headquarters and Headquarters Company, 780th MI Brigade (Cyber)

The Army's Cyber Enterprise is continuing "to boldly go where no one has gone before." We have pushed the envelope in developing the equipment and people to embark in the new cyber environment. The 780th Military Intelligence (MI) Brigade has stood at the forefront of this journey. We have built world-class facilities that enable the brigade to conduct operations, execute training, and sustain our force. We have trained our force and will be the first military Service to have all of our cyber teams achieve full operational capability (FOC) status by the end of this fiscal year. Yet, we are still at the beginning of this new voyage in the cyber domain. In the 780th MI Brigade, our Soldiers, Department of the Army (DA) Civilians, and contractors are the most valuable resource. The brigade's people are what make this unit so effective and dangerous. Therefore, we must ensure that the foundation of our voyage is in the mindset of our people. To continue thriving in the cyber domain, we must remain willing to learn.

We are in an environment that rewards those that continue to learn and adapt. For when we overcome the current challenge, another challenge is ready to come forth from the shadows. Although we have pushed the envelope in the cyber domain, we must realize that we have just begun our journey in this new and exciting domain. There are many unknowns; things we have not considered or have not thought about in this realm. We have to remain open to new ideas, new ways of seeing the cyber environment. Each of us possesses specialized skills that enable us to look at things differently. This perspective enables us to learn from one another and understand the situation at hand. We must learn from our past endeavors and be willing to change where we need to change. This requires us to be humble.

The Soldiers, DA Civilians, and contractors in Headquarter and Headquarters Company (HHC), 780th MI Brigade exemplify the willingness to learn and the desire to push the envelope. HHC personnel, the Honey Badgers, have pushed themselves past their comfort zone and past the normal way of doing things. The cyber domain required HHC personnel to look at things differently, to learn new ways of accomplishing the mission and supporting the brigade commander's priorities. Honey Badgers have kept their edge by remaining humble and learning new ways of supporting the mission. HHC personnel have applied their expertise in their field of study in new ways in order to support the mission. Obtaining new equipment in unique and unconventional methods. Setting up and maintaining the multiple networks that our brigade needs for communication and operations. Working through the security processing in different ways to get our personnel the accesses they need. Analyzing the structure and strength of our personnel throughout the organization to better man our brigade. Solving the unique challenges with supporting cyber from a special staff point of view. And the hard work behind the scenes from the orderly room that works diligently to minimize distractions for the staff so that they can focus on supporting the brigade and its mission. This hard work from the staff sets the brigade up for success. Nevertheless, it must be an adaptable organization made up of personnel willing to learn in order for it to continue to grow and thrive in the voyage within the cyber domain.

The cyber domain is a difficult domain. However, if we are willing to learn every day, we will continue to push the envelope. To continue to push ourselves to be better while remaining humble to realize that we do not know it all and there are thing that we will not know, at least for now. We must remember what James T. Kirk stated – "You know the greatest danger facing us is ourselves, an irrational fear of the unknown. But there's no such thing as the unknown – only things temporarily hidden, temporarily not understood." A willingness to learn will set us on the path to understand these unknowns and to continue our pioneering spirit in the cyber domain. Our willingness to learn will enable us to be "Everywhere and Always, In the Fight."

Honey Badger 6

The Enterprise

By: Frank Colon, attorney, 780th MI Brigade (Cyber)

Following the Brigade Commanders direction to discuss the Army Cyber Enterprise and a recent gift from a friend of a book published in 1917 "The History of the U.S. Navy from the revolution to date" I found myself reminiscing. As a retired Naval officer I decided to compare the history of the ships named Enterprise with that of our burgeoning mission and relatively early placement in the history of cyber.

In 1775 the Continental Navy commissioned the first ship to carry the name Enterprise. Since 1775 seven

Ships Named Enterprise: for more than 240 years, they've boldly served America's Navy – The first Enterprise was originally a British ship named George. (Photo courtesy of USS Enterprise CVN 65's official website)

ships have carried the name USS Enterprise: (1799), a sailing vessel that fired the first shots in the First Barbary War: (1814), a steamboat that participated in the Battle of New Orleans: (1831-1874) a sailing vessel: (1938–1947) an aircraft carrier that served in World War II: (1961–2013) (CVN-65), a nuclear-powered aircraft carrier: (CVN-80), third ship of the Ford class of aircraft carriers scheduled to be constructed and in operation by 2025.

For 250 years, the United States Navy has maintained a ship named the Enterprise. The Cyber Enterprise has been around for less than 40 years, and the Army Cyber Enterprise even less time. That places us somewhere between the (1799) sailing vessel and the (1814) USS Enterprise steamboat. In those 40 years, the Cyber Enterprise now has an estimated 12 billion connected devices. In 2025 when the newest USS Enterprise comes online, the worldwide web will host 35 billion devices including the USS Enterprise (CVN 80) and everyone onboard. Our Brigade just like the crew of the pre nuclear USS Enterprise is at the beginnings of the Army Cyber Enterprise history.

Can you imagine if we were to transport the crew of the 1814 USS Enterprise steamship to the flight deck of the 2025 USS Enterprise with hundreds of servers, thousands of miles of fiber optic cable, touch screen bridge controls that control two nuclear power plants that power a flight control tower launching unmanned combat aircraft on electromagnetic catapults. We are at the early stages of the Army Cyber Enterprise and can only imagine those who assume our role will see and do to ensure the defense of our Nation.

The Army Cyber Enterprise will be as essential in the continued success of our great Nation as the sailors over the years who served the USS Enterprise. Just as the 1814 Enterprise crew could not have known how important each member's efforts were to ensure the success of our Nation, each of our efforts today will ensure the safety and security of our children and grandchildren in the years to come. Without any doubt, the 780th Military Intelligence Brigade (Cyber)'s legacy, name, and members are part of an enterprising effort that only when we work together to form the Army Cyber Enterprise, we ensure the legacy of the 780th will be as enduring as the 250 plus years of the USS Enterprise.

Getty Images

Building Hope & Resiliency: Addressing the Effects of Sexual Assault

A self-guided educational program

What is Building Hope & Resiliency: Addressing the Effects of Sexual Assault?

Building Hope & Resiliency: Addressing the Effects of Sexual Assault is a self-guided, online, educational program that seeks to help individuals begin to recover, heal and build resiliency after a sexual assault. The development of this educational program was directed by the Secretary of Defense in 2015 to meet the needs of the Department of Defense (DoD) community, including cadets and midshipman, who may have been victims of sexual assault or abuse prior to entering military service.

Recognizing the impact that trauma can have on an individual, this program is part of a comprehensive effort to enhance individual and collective resilience and improve readiness across the Total Force. The DoD Sexual Assault Prevention and Response Office (SAPRO), via a contract with the Rape, Abuse and Incest National Network (RAINN), developed and deployed this anonymous, self-guided educational program.

> **Approximately 10% (556 reports) of Service member victim reports involved incidents that occurred prior to military service** (DoD Fiscal Year 2016 (FY16) Annual Report on Sexual Assault in the Military).

Building Hope & Resiliency leverages RAINN's 20 years of experience in providing direct services to survivors and incorporates current research on resilience and strengths-based perspectives to support those using the program as they work to restore resiliency and hope.

What are the goals of *Building Hope & Resiliency*?

- Validate the struggle and adversity that individuals who have experienced sexual assault face.
- Empower users in their healing journey.
- Build knowledge of exercises that can enhance a user's ability to cope with the short- and long-term effects of sexual assault.
- Increase awareness and understanding of, and access to, available mental healthcare resources
- Inspire hope for continuing personal growth.

What can a user expect when participating in the program?

The program consists of five modules and is designed to be completed at the user's pace. The user can decide when they want to access the program and how long they wish to spend on each module.

The modules feature definitions, helpful information about coping mechanisms, practical relaxation exercises, and links to resources and referrals for on-going support. Also included is a brief, optional self-assessment for users to gauge how effective their current coping strategies are and whether they may benefit from additional support and resources.

How can a user access the online program?

Users must create an account, but the program can be accessed anonymously both on a computer and on a mobile device.

- To access the program on a computer a user can visit the Building Hope page on the Safe Helpline website https://www.safehelpline.org/building-hope-and-resiliency.
- Users that use the Safe Helpline app can also access the online program directly through the app page titled Building Hope in the "Learn" section of the app. To learn more about the Safe Helpline app and how to download it to your mobile device visit https://www.safehelpline.org/about-mobile.

For more information visit https://www.safehelpline.org/building-hope-and-resiliency or download the Info Paper.

Equal Opportunity Concerns or Grievances

By: Sgt. 1st Class Eric Frock, Equal Opportunity Advisor, 780th MI Brigade (Cyber)

Soldiers in the Army have two avenues of approach to express their equal opportunity concerns or grievances. This is accomplished by filing either a formal, or informal Equal Opportunity complaint.

Informal Complaint

An informal complaint is one that usually revolves around an isolated incident or something that can be addressed at the lowest level. For example, a Soldier uses a racial slur during a conversation, and a bystander hears the conversation. This is of course prohibited in the workplace, and as a Soldier, and in this case the bystander (or anyone in the conversation) would have grounds to file a complaint. One avenue the person could take is filing an informal complaint.

An informal complaint is one made with the unit's Equal Opportunity Leader (EOL). The EOL will document the incident in a memorandum and usually inquire how the Soldier would like it handled. Often times an incident can be addressed by simply confronting the individual who committed the offense, and letting them know they were acting inappropriately. The EOL will then send the informal complaint to the Equal Opportunity Advisor (EOA) for entry into the Equal Opportunity Report System. The complaint will also be taken to the unit commander but no action will be initiated based off an individual informal complaint unless the commander deems it necessary.

Formal Complaint

The second type of complaint is a formal EO complaint. Any person who is the subject of an incident of discrimination based on race, color, gender (sex including transgender), sexual orientation, national origin, or religion can result in a Soldier filing a formal EO complaint. Any single incident, including the example above is eligible.

A formal EO complaint is made directly with the Brigade EOA. Upon receiving the formal complaint the brigade EOA will notify the brigade commander who will have three days to notify their general courts martial convening authority, as well as assign an investigating Officer (IO). The IO will have 15 calendar days to complete the extension, and up to 45 if an extension is requested by the IO. As in the case of the informal complaint, the EOA will ask what the expected result of the complaint is and try to work with the Soldier and Commander to accomplish those desires.

If the complainant is not happy with the process or the investigation, they may file an appeal once it is complete. Note that the appeal is strictly with the process, and not the results or any punishment the perpetrator does or doesn't receive.

For questions regarding either type of complaint contact the brigade EOA (information below).

If you need to reach me for any reason please call my office at comm: (301) 833-6412, bb: (301) 974-2763, or email me at eric.d.frock.mil@mail.mil. If I do not answer when you call, I will get back to you as soon as I am able. I am located in the Annex trailer at 310 Chamberlin Ave. on Fort Meade, Maryland. In addition, you can contact your unit's Equal Opportunity Leader for assistance.

Making Room for Others...

By: Chaplain (Maj.) Gregory McVey, chaplain, 780th Military Intelligence Brigade (Cyber)

Elevators are odd places, especially crowded ones. You're strangers packed like sardines. You really try not to touch each other. Nobody talks and you can't look at anyone; in fact, you don't look anywhere except up, watching the numbers light up.

Back in May, my family and I took a trip to Virginia Beach. One day, my son and I were waiting for the hotel elevator (which can sometimes seem like eternity). The door opened and it was immediately clear is was full of people, and each person in the elevator gave us that, "hey-you-guys-aren't-gonna-try-to-get-in-are-you look?" I stepped on first, followed by my son. When he stepped aboard there wasn't room enough for him to turn around. As the door slid shut behind him, he smiled big and said loudly, "You might have wondered why we called this meeting today!" The place broke up with laughter. An eleven year old broke the ice. It was the most amazing sight to watch. People actually began talking to each other.

In many respects that elevator is a microcosm of our world today: a large, impersonal institution where anonymity, isolation, and independence are the uniform of the day. It shows us that people can be surrounded by other people in a crowded setting, and not experience community. We can be a part of an organization or group and not feel we belong or are accepted. We can share an office or workspace, and even a home and not have significant relationships.

That was not the case with the Apostle Paul. Wherever he went he established a band of people who huddled together in supportive and encouraging community. How was he able to create significant relationships? First Thessalonians, chapter two, identifies some of the key components for establishing and maintaining community. When we make room for others in our lives the walls of indifference and apathy come down. When we make room for others we discover the best of others and the best in ourselves.

When Gene Stallings was an assistant football coach under the legendary University of Alabama coach, Paul Bear Bryant, a Fellowship of Christian Athletes (FCA) chapter began on the campus. Stallings was the first assistant to attend the meetings. After Stallings had taken the head coaching position at Texas A&M University, he received a call from Bryant, "Stallings, you know what is the worst thing that has happened to our football team? It's the FCA. Those players are doing nothing but hugging on one another, kind to one another, and they won't hit anybody. I need them to hit!"

After the season, which turned out to be one of the best that Bryant ever had, the Bear called Stallings again. "Stallings, you know what is the best thing that has happened to our football team? It's the FCA. It has brought such a oneness and closeness to our team. We were unified because of the influence it had on our squad."

What happened for the University of Alabama football team, what happened in the elevator with my son can happen anywhere. People need each other. We need to take off our masks, admit our need for each other, cultivate relationships, and strive for authenticity.

FORT GEORGE G. MEADE, Maryland -- Pictured are members of the 780th Military Intelligence (MI) Brigade SHARP team, and the "Amazing Race" competitors from: 781st MI Battalion; E Company, 782nd MI Battalion; and HHC, 780th MI Brigade. The race focused on team members working together to gather information that addressed sexual harassment or assault issues they might observe. In addition to the two brigade teams, other teams from across the installation took part in this "amazing race" format on April 27 to advance their knowledge and action in this important area of readiness and preparedness. (U.S. Army Photo)

Respect the Power of Electricity

By George Lawler, Safety Specialist, 780th Military Intelligence Brigade

Electrical safety is critically important in all aspects of life and everyone in the Army Family is reminded to stay aware of potential hazards and understand the importance of electrical safety at home and your workplace.

Many electrocutions and fires can be prevented simply by understanding basic electrical safety principles and adhering to safe practices. Whether you are at home or work, electrical safety should be a top priority. Awareness of electrical hazards is the key to reducing the staggering number of electrically-related home fires, injuries and deaths that occur every year.

Keep these important electrical safety tips and information in mind to protect your home and your workplace.

Prevent Electrical Overloads - Overloaded electrical circuits and electrical equipment in poor repair are responsible for countless fires. Every year scores of people are injured in and around their homes by unsafe conditions that result from a faulty electric breaker panel. Unsafe conditions, such as overloaded circuits and worn or damaged insulation are often the main causes of fires and electrocutions. Keep an eye out for warning signs of overloaded circuit.

- Do not attempt to draw power in excess of the rated capacity for the electrical system
- Make sure all major appliances are plugged directly into a wall receptacle outlet
- Never use extension cords or multi-outlet converters for appliances
- Only plug one heat producing appliance into a receptacle outlet at a time

Use Extension Cords Safely - Extension cords can overheat and cause fires when used improperly. A heavy reliance on extension cords is an indication that you have too few outlets to address your needs. Also be aware that power strips only add additional outlets; they do not change the amount of power being received from the outlet. Keep these important tips in mind when using extension cords.

- Make sure extension cords are properly rated for their intended use, indoor or outdoor, and meet or exceed the power needs of the device being used
- Have additional outlets installed where you need them
- Don't attempt to plug extension cords into one another

Use Ground Fault Circuit Interrupter (GFCI) protection - A GFCI is an inexpensive electrical protection device that can either be installed in your electrical system or built into a power cord to protect you from severe electrical Shocks. GFCIs have played a key role in reducing electrocutions and could diminish thousands of electrical burn and shock injuries still occurring in and around the home each year. Portable GFCIs are also available to provide on-the-spot ground fault protection even if a GFCI is not installed on the circuit.

How Do They Work? - A GFCI constantly monitors current flowing through a circuit. If the current flowing into the circuit differs by a very small amount from the returning current, the GFCI interrupts power in a fraction of a second to prevent a fatal dose of electricity. GFCIs are designed to operate before the electricity can affect your heartbeat. Here's an example: A bare wire inside an appliance touches its metal case. The case is then charged with electricity. If you touch the appliance with one hand while another part of your body is touching a grounded metal object, such as a water faucet, you will get shocked. If the appliance is plugged into an outlet protected by a GFCI, the power will be shut off before a fatal shock can occur.

Electrical work is inherently dangerous. Professional electricians receive years of training and on-the-job experience before the state grants them a license. Use discretion when attempting your own electrical work. To make sure all the electrical systems in your home are safe, up to code and working as they should, hire a trusted electrician to handle the job. Facility Managers are the assigned unit's primary point of control and signing authority for work requests and related financial obligations

Remember, electrical safety is everyone's business!

References and sources:

Electrical Safety Foundation International

Occupational Safety and Health Administration

Stay Everywhere and Always...In the Fight!

I, _____, do solemnly swear (or affirm) that I will support and defend the constitution of the United States against all enemies, foreign and domestic; that I will bear true faith and allegiance to the same; and that I will obey the orders of the President of the United States and the orders of the Officers appointed over me, according to regulations and the uniform code of military justice. So help me God!

780TH MILITARY INTELLIGENCE BRIGADE RETENTION TEAM

Senior Career Counselor
Sgt. 1st Class Scott R. Morgan
Commercial: 301-833-6405

781st Military Intelligence Battalion
Career Counselor
Staff Sgt. Kevin Standring
Commercial: 301-677-4088

782nd Military Intelligence Battalion
Career Counselor
Sgt. 1st Class Pamela Green
Commercial: 706-849-4675

FORT GEORGE G. MEADE, Maryland – Lt. Gen. Paul Nakasone, commander, U.S. Army Cyber Command (ARCYBER) (right), introduces Gen. James McConville, Vice Chief of Staff (VCSA), U.S. Army, to Sgt. Maj. Jesse Potter, operations sergeant major for the 780th Military Intelligence (MI) Brigade, outside the brigade headquarters, August 10. The VCSA was here to receive updates from ARCYBER, 780th MI Brigade, the Cyber Protection Brigade, 1st Information Operations (IO) Command (Land), and U.S. Army Network Enterprise Technology Command (NETCOM), on the Army's capabilities in Offensive Cyberspace Operations (OCO), Defensive Cyberspace Operations (DCO), Department of Defense Information Network (DODIN) operations, cyber initiatives, Cyber Electromagnetic Activities (CEMA), and IO. (U.S. Army Photo)

FORT GEORGE G. MEADE, Maryland – Gen. James McConville, Vice Chief of Staff (VCSA), U.S. Army, presented VCSA coins to Army specialists David Newkirk, Headquarters & Headquarters Company, 780th Military Intelligence (MI) Brigade, and Eric Robbins, Grant Ward, and Tyler Marden, of C Company, 781st MI Battalion, 780th MI Brigade, at the brigade annex here, August 10. (U.S. Army Photo)

Cross Pollination of the Cyber Force

Continued from page 4

Cyber Command and CYBERCOM to better align with the Army's unified cyber approach.

The second approach is the movement of cyber Soldiers between the Cyber Protection Brigade, headquartered at Fort Gordon, Georgia, and the 780th Military Intelligence Brigade, at Fort Meade. This effort is now underway with the movement of key senior NCOs across both formations. Furthering this effort, as junior cyber Soldiers graduate from Phase 2 of their training in August they will begin a balanced cyber career path that enables movement between the brigades and focus areas thereby building a balanced cyber warrior of the future. Like our maneuver brethren, there is no offensive and defensive infantryman, the future cyber warrior will be an expert from both perspectives.

For many who still doubt this approach I leave you with one final example: An Exploitation Analyst identifies system and network vulnerabilities and develops access and reconnaissance strategies that enable the execution of cyber operations. The Cyber Defense Analyst understands, detects, and emulates adversary techniques defending against physical or logical access to network components from both a host and network perspective. I would challenge someone to prove that a cyber Soldier who identifies network and system vulnerabilities in adversary systems would not excel at protecting a system from an adversary from exploiting those same vulnerabilities.

Cross-pollination of the Cyber Force is crucial to developing the balanced cyber warrior the Army envisioned back in 2014 when the CSA directed the establishment of the Cyber Branch and creation of CMF 17. This approach builds on our Signal and MI backgrounds, enabling future cyber warriors to achieve a truly balanced maneuver focused approach to cyberspace operations.

Cyber Civilian Deploys...

Continued from page 10

I mentored and provided training on certain databases that would enhance their analysis. At the same time, I was tasked to provide cyber support to the TF and USCYBERCOM. My days consisted of looking at

TF/USCYBERCOM priorities, conducting analysis, and providing my findings to Chief Warrant Officer Scott Clark, the senior cyber planner, and fellow 781st MI Battalion, *Vanguard* teammate. In turn he would package the findings and recommend effects to the TF and USCYBERCOM.

Success came by completely integrating into the TF, providing them their first experience with cyber support, and helping them to realize that cyber could indeed provide support to kinetic strikes. The success was evident as evidenced by the TF requesting replacements for both Chief Clark and I. If the main mission was to ensure that the TF saw the value of cyber support to their operations, then we accomplished the mission! We were able to accomplish other milestones too – while deployed, Chief Clark and I were able to help create a concept of operations (CONOP) that was designed to help degrade the targets through cyberspace operations. The operation was a success, and it received laudatory comments from the TF and JSOC CDR.

The accomplishment of the mission was a team effort. I could not have done as well as I did if it was not for Chief Clark. He had deployed before so he knew how things went. He was aggressive and never took no for an answer. He always looked for ways to get to 'yes' and in doing so, he enabled both our successes. I highly recommend that cyber professionals deploy forward, and provide cyberspace operational support to the war fighter. It is an extremely challenging and fulfilling mission. You certainly will not regret it! --

-- Pedro

Joint Integration and Partnerships

Continued from page 15

developing the MDB concept. MDB is paradigm shift from traditional Land and Air battle doctrine, includes all domains and all resources to create "Windows of opportunity by creating dilemmas for the enemy." CEMA (Cyber Electromagnetic Activities) Support to Corp and Below (CSCB), plays a large part in creating doctrine where a Joint and or Multinational Force Commander can no longer expect to have instant dominance through all domains. In this case, dominance in cyberspace, requires our forces to operate in an environment where our adversaries meet or, potentially, surpass our capabilities to deliver effects in and through cyberspace. Detachment Hawaii leaders have invested a tremendous amount of effort educate USARPAC senior leaders while partnering with their staff leads to better understand Cyberspace Operations. The ability to influence our senior leaders is a testament to their ability to understand the progression of warfare, while placing spotlight in the tremendous value cyberspace warriors bring to the fight.

As the only Army cyber unit in the USPACOM AOR, Detachment Hawaii benefits from the exposures of our Joint Partners, a Combatant Command Headquarters, and more traditional Army formations. These exposures not only provide opportunities to get after our mission but give our Soldiers, Civilians and even families a level of experiences not seen by another Army Cyber Mission Force. More than a tropical paradise, an assignment to Hawaii and Detachment-Hawaii is a professional and personal opportunity of a lifetime.

"KOPIANA! Search and Destroy"

131As in the Cyberspace Domain

Continued from page 16

carefully selected for the Cyberspace positions because not all 131As have the ability to perform well in an environment such as this.

To build upon the strongest in the 131A Corps, rotational assignments through cyber assignments, and back to FORSCOM, is paramount to understanding and incorporating this new domain into mission planning with realistic expectations. This should be done with a Chief Warrant Officer 2 or 3 that shows high potential being brought into CMT positions for basic level introduction into this domain, whereas a Chief Warrant Officer 3 or 4 that has shown remarkable talent as a brigade or division Targeting Officer should be placed in a JFHQ position. This allows a Chief Warrant Officer 2 or 3 to understand the nuances of the domain and take this information back into FORSCOM upon their PCS, whereas a Chief Warrant Officer 3 or 4 in a JFHQ position can focus more on the compiling and presentation of targets to a COCOM while assisting in those targets integration onto a target list and eventually onto the Target Synchronization Matrix (TSM). Senior 131As should remain at the component and higher echelons to provide oversight and a voice for the 131A community. The integration of 131As into the cyberspace domain has allowed for a new domain to be analyzed and developed to support the warfighter by a professional that is responsible for evolving the battlespace to provide the warfighter with an advantage over our adversary; much like a battlefield, 131A positions and understanding of the domain will continue to evolve while we add another specialty to our subject matter expertise.

This is the end of the BYTE: 780th Military Intelligence Brigade - turn the magazine over to read more!

Volume 5, Issue 4

the BYTE

Cyber Protection Brigade

* Exercise Eager Lion
* CEMA Support to Corps and Below
* CPB Hacks the Air Force
* Partnering with USAFRICOM

OMNES IRE

The Army Cyber Enterprise

The BYTE is a publication of the 780th Military Intelligence (MI) Brigade, Fort George G. Meade, Md.

The BYTE is an official command information publication authorized under the provisions of AR 360-1. The magazine serves the service members and Department of the Army Civilians (DACs) of the Cyber Protection Brigade (CPB), and their Families.

Opinions expressed herein do not necessarily represent those of the CPB, or that of the Department of the Army.

All photographs published in the BYTE were taken by the CPB, or their Family members, unless otherwise stated. The front cover and graphic posters contained within the BYTE were created by the previous 780 MI Brigade public affairs officer (PAO), Tina Miles, or Steven Stover, unless otherwise stated.

Send articles, photographs or story ideas to the 780th MI Brigade PAO at steven.p.stover.civ@mail.mil, or mail to 310 Chamberlin Avenue, Fort George G. Meade, MD 20755.

For additional information, call (301) 833-6104.

Col. Paul T. Stanton
Commander

Command Sgt. Maj.
Jack Nichols
Command Sergeant Major

CONTENTS:

In every issue...

On the cover: Army Cyber Protection Team members use PlanX at a recent surge week, one of the development methods used to create and improve the system. First used by software and system developers in Silicon Valley, surge weeks are designed to gather user feedback about system functionality. (U.S. Army photo)

Commander's Column

By Col. Paul Stanton, commander, U.S. Army Cyber Protection Brigade

As we continue to tackle challenging defensive missions within the Cyber Protection Brigade (CPB), I have paused recently to ask, "What about the Army CPB uniquely postures us to execute these missions?"

Given the expertise and capabilities of a $7B commercial cybersecurity industry, why is the Army engaged in defensive cyber operations (DCO)? My answer is simple: the Army is good at warfighting.

Ultimately, warfare is a battle of wills where the victors force opponents to change their aims. In defensive cyber operations, an objective is to increase the opponents' resource cost to the point that the enemy must abandon his goals. We focus the defense of critical assets to make the enemy's expenditure and investment in capabilities, time, manpower, and money exceed the threat's capacity. A successful cyber defense forces the threat to abandon aims and capitulate in the battle of wills. Fundamentally, then, defensive cyber operations are a form of warfare.

Given this context for defensive cyber operations, the U.S. Army is really good at planning, leading, and training for war. As Army Cyber defenders, we must capitalize on this expertise to prepare for, structure, and execute cyber defense. The Army's warfighting expertise is the distinguishing characteristic that makes the Cyber Protection Brigade relevant.

The Army is really good at planning. So too, must the CPB employ the military decision making process anchored in mission analysis, course of action development, and operational orders to develop a tactical cyber defense. The process of gathering and synthesizing relevant information in the context of mission objectives is inherent to Army planning. As cyber defenders employ the same practices, the process provides the necessary focus to orient the defense on prioritized assets where we can provide mission assurance and impose the greatest cost on the enemy.

The Army is good at leading. We build adaptive leaders of character who embody the Army Values and can operate decisively in complex, uncertain, and ambiguous environments. Nowhere are these leadership traits more relevant than within cyber operations. The complexity and continuous evolution of technology is overwhelming; mission success requires rapidly synthesizing data, assigning tasks, issuing intent, and empowering subordinates to execute. Leaders must remain abreast of the situation and make decisions in a dynamic environment. They must align resources and combat power to reinforce success at critical moments during mission execution. Leadership in defensive cyber operations through the Army's concept of mission command is the critical enabler.

The Army is good at training for warfare. Highly skilled, adept, and technologically sound warfighters are not inherent to the workforce. The Army must develop the individuals and teams through rigorous education and training. In cyber operations, education is foundational, but, by itself, insufficient. Operators must clearly understand the technology, but they must also be able to combine individual efforts toward common objectives at mission relevant speed. This requires training. Teams of subject matter experts must synergistically integrate individual tasks into collective tasks oriented toward mutually supporting objectives. The Army has instituted training models across all maneuver elements to gain the required proficiency for mission success. Defensive cyber operations must follow.

As cyber continues to evolve as a warfighting domain, we must capitalize on the Army's proficiency at warfighting. As we manage technical complexity, we must stay grounded in the fundamental principles inherent to our profession as Army leaders. We must combine our skills as warfighters with our skills as computer scientists, network engineers, and analysts to continuously raise the cost to the adversary and force him to abandon his aims. This combination of skillsets makes the CPB not only relevant, but necessary.

Omnes Ire!

The Ever-Evolving CPB

By Lt. Col. Aaron Gould, executive officer, Director of Strategic Initiatives, U.S. Army Cyber Protection Brigade

The U.S. Army Cyber Protection Brigade (CPB) has undergone a substantial transition in the last year. And what a year it has been for the Department of Defense's (DOD) premier Defensive Cyberspace Operations (DCO) team!

When the Army activated the CPB in 2014, the brigade's primary mission was to build Cyber Protection Teams (CPT) – to man, train, and equip CPTs to reach their Initial Operational Capability (IOC) and Fully Operational Capability (FOC) gates on prescribed timelines. While the cyberspace defenders set out to execute an orderly build process for our DCO forces, our adversaries had other plans. Those plans included continuously and relentlessly targeting the DOD's networks, systems, and data in the pursuit of nefarious objectives.

To deal with complex global threats in cyberspace, the CPB was forced to accelerate a number of ongoing transformations. First and foremost, a fundamental culture shift was in order. If our adversaries were on the offense (they still are!), we couldn't afford to remain primarily focused on the build process. So, after an incredibly successful two-year build phase, Col. Paul Stanton, the brigade commander, and Command Sgt. Maj. Jack Nichols, the brigade's senior enlisted Soldier, made a calculated push to change the organization's mindset. We desperately needed to move beyond the "Build the Brigade" mentality and embrace a more aggressive culture focused on "Operationalizing the Brigade." To signify this shift, the CPB adopted a new mission statement:

*Cyber Protection Brigade defends **key terrain** against **specified threats** to **deliver effects** that ensure freedom of action in and through cyberspace and to deny the same to our adversaries.*

The new mission statement conveys the operational focus, and is now the guiding principle behind every endeavor the CPB embarks on. The formation responded magnificently and has consistently remained well ahead of mandatory IOC/FOC build timelines, while defending key terrain all over the world in support of the Army, the Cyber National Mission Force, the Defense Information Systems Agency (DISA), and the Combatant Commanders.

To truly operationalize the CPB, however, another major change would be required. The best way to fight agile, tailored DCO teams to deliver effects at the right time and place, was to afford the CPB commander operational control (OPCON) of his CPTs and mission elements. The U.S. Army Cyber Command (ARCYBER) commanding general agreed, and earlier this year Lt. Gen. Paul Nakasone delegated operational control of the Army's Service CPTs to the CPB Commander.

Assuming OPCON of such a dynamic organization heavily engaged in high-stakes operations across the globe, with the original CPB organizational structure, was not a trivial undertaking. The original design called for a CPB headquarters and twenty CPTs, with no intermediate command and control (C2) structure between the brigade commander and the CPTs. Needless to say, this was not a good model for the OPCON approach. The commander and his staff conducted detailed analysis and developed a sound plan to effectively take on the new OPCON role. The principle challenges centered on the lack of intermediate C2 structure and a host of enabling capabilities. To overcome these challenges, the CPB recommended an organizational

Continued on page 12

Soldiers from 1st Cyber Protection Battalion defend CyberTropolis during the Jailbreak exercise at the Muscatatuck Urban Training Center in Butlerville, IN. Pictured: PFC James Olds, CW3 Charles Frierson, SFC Carl Whitaker, CW2 Joshua Neely, and SSG Anthony Striano. (U.S. Army photo)

CPB Improves Readiness via Innovative Gunnery Program

By Lt. Col. John Hosey, Headquarters, U.S. Army Cyber Protection Brigade

The kinetic maneuver world (Field Artillery, Infantry, Aviation, etc.) have been utilizing the gunnery methodology and gunnery tables for hundreds of years; such as Napoleon's artilleryman utilized gunnery tables to ensure more accurate fire. This doctrine has matured over the years to encompass not only the accurate fires, but also the training to utilize the assigned weapon system, how to utilize the combined systems as a cohesive crew, and

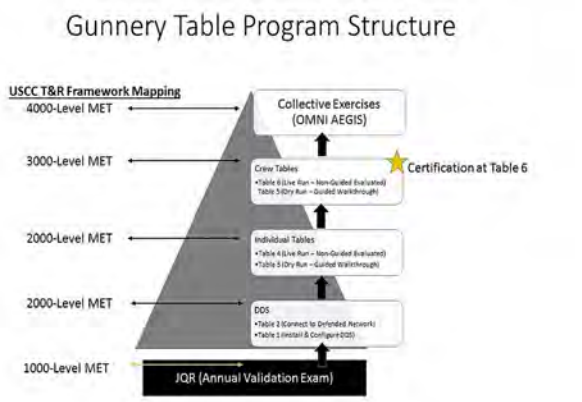


Figure 1 DCO Gunnery Tables mapped to USCC Training and Readiness Requirements.

then finally as larger sized elements. With Cyberspace as the newest domain of war, the Cyber Branch was created to be the maneuver forces that operate in and through it.

The U.S. Army Cyber Protection Brigade (USCPB) has taken the concept of gunnery a generation forward by incorporating gamification into DCO Gunnery. Partnering through the Program Executive Office Simulation, Training and Instrumentation (PEO-STRI)

with a private vendor, the USACPB has developed a training platform, Project Sparta, which allows the brigade, battalion, and cyber protection team leadership to objectively assess crews and develop tailored training plans for each cyber warrior. This platform engages the cyber workforce through familiar gamification concepts, such as leaderboards and skill badges. Collectively these game artifacts have the added benefit of populating a repository for talent management of the newly established defensive cyber forces.

The USACPB has been developing the DCO Gunnery tables for the past year and has recently published several tables to initiate training and instruction. The brigade has also tested the concept with sister Services and United States Cyber Command; both are looking at utilizing the training concepts and the platform in the joint environment.

Members of 2nd Cyber Protection Battalion pose for a team photo while supporting a named operation at a forward location. (U.S. Army photo)

CPB Cyber Support to Exercise Eager Lion

By Capt. Brad Hitchens, 100 Cyber Protection Team, U.S. Army Cyber Protection Brigade

The Background

Eager Lion is an annual multi-national combined arms exercise hosted by Jordan, and organized by United States Central Command (USCENTCOM) and the Jordanian Armed Forces. In 2017, more than 20 countries participated in the exercise.[1] A newly established, closed exercise network presented an opportunity for expanded Cyber Mission Forces (CMF) participation.

USCENTCOM had two primary cyber-related goals for Eager Lion 2017. The first was to build partner capacity by providing an opportunity for the Jordanian Computer Emergency Response Team (CERT) and participants from other partner countries to train and exercise their incident response plans. The second goal was to exercise the Combined Joint Task Force's (CJTF) ability to operate in a constrained environment with degraded communications.

Preparation – Inject Development

The USCENTCOM J-6 tasked 100 Cyber Protection Team (CPT) to develop and run the cyber injects for the exercise. The exercise scenario featured a moderately skilled trusted insider with standard user access who was covertly working on behalf of a foreign government. While developing injects for the exercise, the CPT members focused on providing injects that created a realistic scenario for the defenders to operate against. The CPT accomplished this using the Cyber Kill Chain[2] as a basic framework, and identified open-source exploits to use against the CJTF's network.

Exercise – Inject Execution and Incident Response

The inject team initiated their efforts by running "loud" NMAP (network mapped) scans against the network to test the CERT's ability to identify attacks and respond. The CERT quickly identified the scans and initiated their incident response plan. Since they were able to quickly identify the scans, the inject team was more subtle with their future injects.

The next inject was a phishing campaign against the CJTF, which was intended to test both the CERT's handling of the incident and the reaction of the CJTF's users. Two separate emails were sent. The first was designed to mimic a standard non-compliance warning requiring the recipients to open and sign an attached acceptable use policy. The attached Word document was built using Metasploit's exploit for the Microsoft Word HTA vulnerability (CVE-2017-0199)[3]. Approximately 10 percent of the recipients opened the attachment, providing the inject team with access into the network. The team sent a second email with an attached Power Point document that directed recipients to run an embedded executable. Despite user warnings after the first phishing email, one user still ran the executable.

The configuration of exercise computers and limitations of open-source privilege escalation exploits forced the inject team to use their insider's physical access to get credentials. The insider used a Linux live disk on a Domain Administrator's computer to replace utilman.exe (accessibility options) with a Meterpreter payload and ran the executable from the Windows login screen. This provided the inject team with a reverse shell with System permissions. The team used this access to enable WDigest from registry, which allowed them to view the Domain Administrators plain-text credentials with Mimikatz.

Using newly obtained administrative credentials, the team moved on to their next inject –exfiltration of data to an FTP server. The CERT identified the unauthorized FTP traffic and requested an IP block at the firewall to prevent unauthorized data exfil. With additional research, local defenders were able to identify many of the stolen files and report this information to the CJTF and the higher headquarters.

The final inject was disruption of CJTF key leaders, intended to test both the CERT's response and the

Continued on page 12

1 https://www.dvidshub.net/feature/EagerLion2017

2 http://www.lockheedmartin.com/us/what-we-do-/aerospace-defense/cyber/cyber-kill-chain.html

3 https://www.rapid7.com/db/modules/exploit/windows/fileformat/office_word_hta

151 CPT Supports "Hack the ERP"

By Maj. Craig Sanders, 151 Cyber Protection Team, U.S. Army Cyber Protection Brigade

Soldiers from 2nd Cyber Protection Battalion conduct operations in support of the Army's "Hack the ERP" program. Pictured are: Sgt. 1st Class Christopher Russell, Staff Sgt. Rodricus Sturgis, Chief Warrant Officer 3 Sonny Navarrette, and Chief Warrant Officer 2 Brandon Larson. (U.S. Army photo)

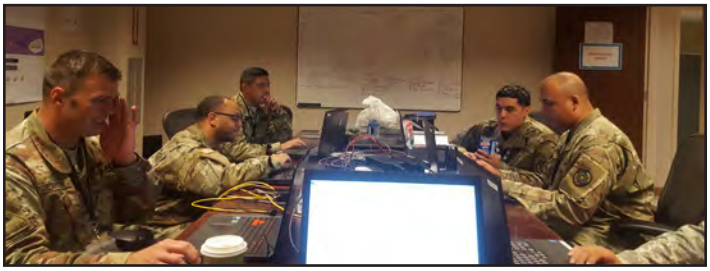
The United States Army Cyber Protection Brigade (USACPB) was selected to defend the Army's Global Combat Support System-Army (GCSS-A) and the Logistics Modernization Platform (LMP) networks and systems infrastructure against out-of-scope and out-of-bound attacks during the "Hack the ERP" event in July 2017.

The CPB employed a seasoned Defensive Cyberspace Operations (DCO) mission element to defend these critical enterprise logistics systems in order to preserve the confidentiality, integrity, and availability of the systems and their sensitive data. The FY17 Hack the ERP event focused on two Army-owned Enterprise Resource Planning (ERP) environments: Global Combat Support System-Army (GCSS-A) and the Logistics Modernization Platform (LMP).

The DoD's computer networks and systems are essential for daily business operations and mission-critical activities. Securing the DoD's networks is a matter of national security that requires the continuous identification and remediation of vulnerabilities that could be exploited by malicious cyber actors. As part of its responsibility to the public at large, the DoD is constantly considering innovative and diverse approaches to protect our critical systems and data.

In order to deal with complex global threats, the DoD must remain at the forefront of rapidly evolving technologies, while also maintaining the highest levels of cybersecurity to protect these new technologies. To address the ever-growing, highly dynamic threat landscape, we must look for new and innovative ways to facilitate vulnerability discovery, coordination, and responsible disclosure. One way the DoD has attempted to improve vulnerability discovery is crowdsourcing – leveraging a diverse pool of information security researchers from the private sector. Along these lines, the Army will sponsor a Hack the ERP initiative using the Defense Digital Service (DDS) contract vehicle with a renowned cybersecurity firm called Synack.

The CPB will establish a defense within the target environments in order to detect and, if directed, prevent anomalous or unauthorized activity. The CPB prepared for the Hack the ERP event by conducting an area reconnaissance of the GCSS-A data center in Redstone Arsenal, Alabama. During the recon effort, the DCO element executed the sensor emplacement plan and occupy observation points using the system owner's organic cybersecurity tools. Actions on the objective during this phase include: 1) validation of existing network maps and vulnerability scans; 2) assessment of current cybersecurity hygiene processes such as Security Technical Implementation Guidelines (STIG) compliance; and 3) development of hardening recommendations to be implemented by local defenders prior to the Hack the ERP event. At the completion of this phase, the CPB mission element was postured to defend against out of bound and out of scope attacks against the GCSS-A enclave. Allowing carefully-vetted security researchers to "Hack the ERP" and disclose identified vulnerabilities will allow the Army to proactively improve the security posture of these critical assets.



Pictured are: Chief Warrant Officer 2 Brandon Larson, Staff Sgt. Rodricus Sturgis, Chief Warrant Officer 3 Sonny Navarrette, Warrant Officer Arsenio Pagan, Staff Sgt. Ruben Vasquez.. (U.S. Army photo)

CEMA Support to Corps and Below

By Chief Warrant Officer 4 Eric Averill, 152 Cyber Protection Team, U.S. Army Cyber Protection Brigade

In 2006, the Army departed from its Cold War divisional orientation to a full-spectrum capability with fully manned, equipped and trained Brigade Combat Teams (BCT). As this reorganization progressed, the United States continued to commit forces around the world. While our nation was immersed in conflict, threats and adversaries developed advanced capabilities within the Cyber Domain. The Department of Defense (DoD) has spent decades tackling this issue as it has risen to the forefront of conventional and unconventional operations. The Chairman of the Joint Chiefs of Staff formally codified the requirement for dominance in the Cyber Domain by directing the creation of the Cyber Mission Force (CMF) in 2014.

The World Class Cyber Opposition Forces (WCCO) of 1st Information Operations Command, have continuously denied, degraded, and disrupted BCT operations using widely published, open-source exploits and methods since 2011. In 2015, Army Cyber Command (ARCYBER) established the Cyberspace and Electromagnetic Activities (CEMA) support to Corps and Below (CSCB) pilot program, to determine how Cyber operations can better enable the war-fighter. Since then, units with CSCB have demonstrated greater resiliency against the WCCO's efforts during major training events. Despite these successes, known system vulnerabilities continue to provide avenues of approach into BCT systems. There are two ways forward for the defense of the war-fighter at the tactical edge, and they lie in the modularity of the BCT and in the assignment of responsibilities within the Cyber domain and across separate components.

BCTs were developed with a modular framework. All BCTs have similar equipment, personnel authorizations, and capabilities. This standardization extends to the BCT's network, with most units deploying similar infrastructure, software, and services to accomplish their missions. For operations across all domains to be successful, DoD components must posture to secure and defend all organic systems, services, and network infrastructures. Understanding that BCT network architecture will be uniform, the U.S. Army Cyber Protection Brigade (CPB) has committed forces to developing a standardized methodology for securing the BCT that, when finished, can be delivered to any BCT as a technique to defend the network with best practices in mind.

Across higher echelons, tactical units, service providers, and CMF components, we must strive to reduce duplicate efforts and clarify cybersecurity responsibilities. The Army's current tactical network construct consists of Regional Cyber Centers (RCCs) providing services through Regional Hub Nodes (RHNs) at the Defense Information Systems Agency (DISA) level to Corps and below tactical units. Delineating the Signal and Cyber responsibilities associated with each component will streamline the Army's operations in the Cyber domain and improve its mission assurance capabilities as the Signal Corps' 255S Cybersecurity Technicians make their way to the larger force.

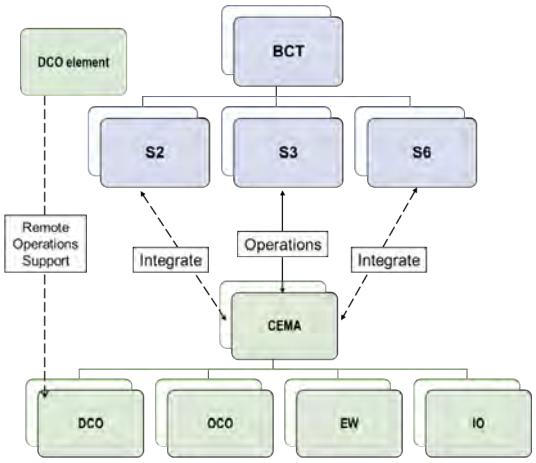


Figure 1. CEMA Support to Corps and Below Construct

Continued on page 11

	Unit Corps and Below	Provider DISA, RCC, RHN	CMF Operations CPT, NMT, CMT
Primary Proactive	1. Secure 2. Retain	1. Interdict 2. Block	1. Counter Recon. 2. Control
Situational Reactive	3. Isolate 4. Neutralize 5. Suppress	3. Contain 4. Canalize 5. Clear	3. Interdict 4. Contain 5. Clear

Figure 2. Proposed Cyber Tasks for Army Components

CPB Hacks the Air Force

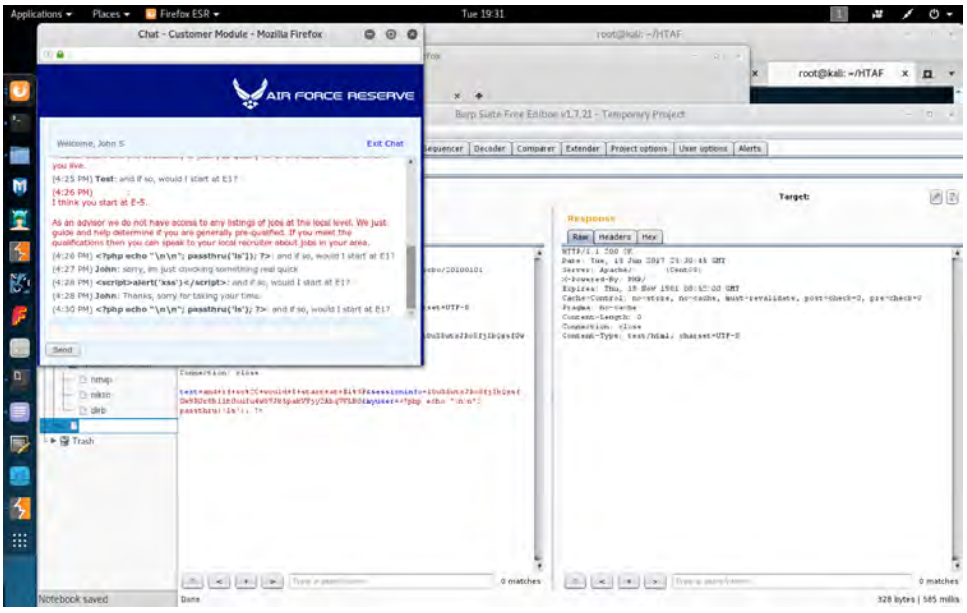
By Capt. Craig A. Laprade, 154 Cyber Protection Team, U.S. Army Cyber Protection Brigade

The call went out late in the evening after most of the Army had closed up shop. US Cyber Command (USCYBERCOM) sent out the call for teams to participate in the "Hack the Air Force" (HTAF) bug bounty. Army Cyber Command (ARCYBER), in turn, tasked the Cyber Protection Brigade (CPB) to field a team of Cyber Soldiers; preparation would start almost immediately. I knew this advertisement piqued the interest of others in the CPB who had a penchant for the hacker mindset. I was eager to submit my name and meet these kindred spirits.

The CPB hacking team consisted of three highly motivated individuals. It did not take long, however, for us to realize that none of us had done this before. Two of the participants were highly trained, but new to the Cyber Mission Force. The third team member was a seasoned network defender, but had never – even in his spare time – changed hats and tried being the attacker. We started by building a Redmine site in an Amazon Elastic Computing Cloud 2 (EC2) instance and setting up a Slack space for chatting (we were new to offensive operations but we were not new to teamwork). We exchanged ideas on how this would play out, but none of us really knew. Most of us have had the experience of using .mil websites in our day-to-day jobs. We were salivating at the opportunity to take a swing at the Air Force sites. All of our hearts sank when we saw the first list of sites published: nothing but .com domains – apparently developed and maintained by skilled professionals. Our expectations went from getting root shells to something much less.

On day one, the team took a crack at the authorized domains. As we had expected, the anticipated .mil-isms were not there and we were looking at commercial sites running a mix of commercial content management systems and front-ends. The quick wins we had anticipated were just not coming in, but the team drove on throughout the week and on Friday, we submitted our first bug. The bug proved to be a combination of information disclosure and unauthenticated access – an odd exploitation of a CMS and Apache not agreeing on when a user has access to certain resources. This win was the ice-breaker we needed.

Progress through the remainder of the event varied, but at the final count, the CPB team had submitted 15 vulnerabilities to the HTAF via Hackerone. Unfortunately, we missed being first on six of these by minutes, because new domains were added to the scope in the middle of the duty day when we were committed to other tasks.



A member of the USACPB hacking team tests the patience of a chat advisor while hunting bugs

The experience was well worth it for all involved. Were we the most lethal red team? Not at all. However, over the course of a few short weeks, all three of us gained a much deeper understanding of the web attack surface area that we are often charged with defending. With this experience under our belt, we will find more bugs next time around, and our lessons learned will help us better defend Department of Defense (DoD) networks. Look out for the CPB during future hacking events!

154 CPT Defends Platform IT Control Systems

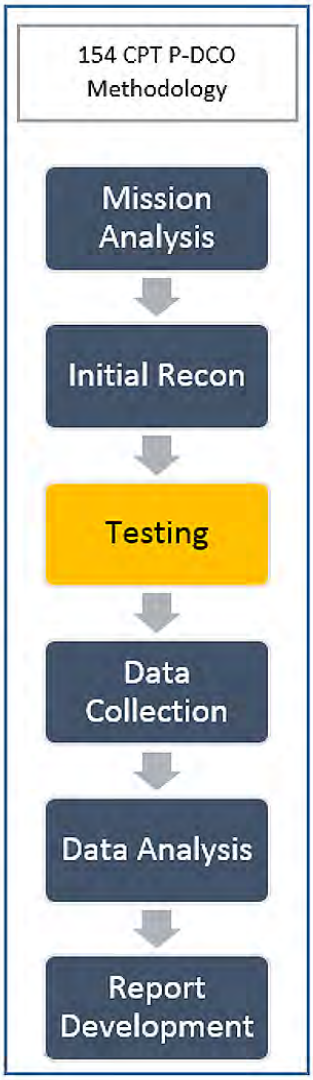
By Maj. Joe Marty, 154 Cyber Protection Team, U.S. Army Cyber Protection Brigade

In response to a far-reaching cyber incident during the summer of 2015, U.S. Army Cyber Command (ARCYBER) deployed 154 Cyber Protection Team (CPT) to the National Capital Region (NCR) to support a major Army Headquarters. That incident response mission laid the foundation for 154 CPT's positive relationship with the supported organization, which led to a continuing partnership on the team's current mission: proactive defensive cyberspace operations (P-DCO) of critical infrastructure on the Department of Defense Information Network (DODIN). 154 CPT (the "Sentinels") attended advanced cybersecurity training for Industrial Control Systems (ICS) and Supervisory Control and Data Acquisition (SCADA) environments, and developed a repeatable methodology to begin effective P-DCO in ICS enclaves. The team's aggressive 90-day mission timeline encompasses mission analysis, pre-deployment site survey (PDSS), testing, data collection, data analysis, and report development.

Soon after the PDSS, the team meets with the Information Assurance Manager (IAM) of the partner organization at a lab to test all of the tactics, techniques, and procedures (TTPs), tools, and methods that will be used on the partner's network. The test week is the most important element of the methodology, and is unique to ICS/SCADA missions. This event doubles as a mission rehearsal for the team, but most importantly it proves how the team will collect all host and network data without disrupting any SCADA operations, and it builds the partner organization's trust and confidence in the team's actions. By the end of the test week, all parties involved in the operation are comfortable with how the mission will be conducted on the SCADA network.

The 154 CPT Sentinels followed, and refined, this methodology through five P-DCO missions in ICS/SCADA environments, referred to within the DoD as Platform Information Technology – Control Systems (PIT-CS) missions. The team shared their lessons learned from these PIT-CS missions at the DCO Conference hosted by U.S. Cyber Command in May 2017, and later traveled to Scott Air Force Base to share their experiences with the Air Force service CPTs. Additionally, the team integrated members from other CPTs (both Army and Air Force) on missions to share its proven ICS/SCADA DCO methodology and TTPs.

The Sentinels started their journey in ICS/SCADA proactive defense at the end of 2015, and have been relentless in their pace since receipt of mission. Collectively, the Sentinels have driven more than 5000 miles over mid-western United States terrain to install enduring network security monitoring (NSM) sensors at 21 facilities over the past 18 months. The team completed five missions through snow, flooding, and tornadoes without causing a single disruption to SCADA operations. Now the Sentinels have begun their sixth mission in defense of the nation's critical infrastructure as the premier defenders of ICS/SCADA systems. 154 CPT team members have learned many lessons, developed new TTPs for defensive activities in ICS environments, and have shared their experiences with the cyber mission force while forging the path in this vital and underserved field of information security. Amid frequent personnel turnover, higher headquarters restructuring, and ever-changing requirements, the Sentinels continue to live up to their team motto of "Elite Defense!"



201 CPT Builds Strong Relationship with USAFRICOM

By Capt. Alisha Garcia, 201 Cyber Protection Team, U.S. Army Cyber Protection Brigade

Staff Sgt. Matthew Malesinski, right, 201st Cyber Protection Team network security analyst, reviews data his team collected during a cyber security audit of the 1st Combat Communications Squadron's tactical communications kits March 16, 2017, on Ramstein Air Base, Germany. (U.S. Air Force photo/Staff Sgt. Timothy Moore)

Over the last 18 months, 201 Cyber Protection Team (CPT) has been extremely busy conducting defensive cyberspace operations (DCO) across three continents and delivering mission critical support to United States Africa Command (USAFRICOM). So far, the team has completed three survey missions to Camp Lemonier, Djibouti in support of Combined Joint Task Force – Horn of Africa (CJTF – HOA); one survey mission to Stuttgart, Germany in support of USAFRICOM Headquarters (HQ); and one survey of an Air Force tactical communications kit for the 1st Combat Communications Squadron in Ramstein, Germany. These missions assisted USAFRICOM in identifying and mitigating threats that would not be uncovered by standard information assurance procedures, in order to improve the security posture for mission essential resources and assets.

Recently, 201 CPT provided a highly trained network technician to conduct a cyber mission assurance assessment in Kenya as part of the USAFRICOM Combined Assessment Team in support of DOD assessment requirements. The team is leading the way in providing increased capability to its combatant command (COCOM) by conducting remote operations from Fort Gordon to USAFRICOM utilizing dedicated SIPRNet and NIPRNet tunnels. The remote connection allows the team to have a constant presence on the AFRICOM network, facilitating rapid, effective, and efficient DCO support.

The team participated in two major exercises conducted by the USAFRICOM HQ. During JUDICIOUS RESPONSE 17, 201 CPT and local cybersecurity defenders defeated all red team attempts to compromise the AFRICOM network. The team received recognition by leaders at all levels for adding critical defensive capability in the protection of cyber domain assets. EPIC GUARDIAN 17 was the first COCOM level exercise to employ two CPTs (200 and 201 CPT) in a coordinated cyber defense, while also using a CPT Cyber Threat Emulation (CTE) squad as the cyber opposition force. The result was a comprehensive training experience for CPT operators and the USAFRICOM DCO community that validated risk mitigation plans that 201 CPT delivered during previous survey missions.

201 Cyber Protection Team, U.S. Army Cyber Protection Brigade, was recognized for success during Judicious Response 17 in Stuttgart, Germany. (U.S. Army photo)

Priority Intelligence Requirements, Indicators of Compro

By Maj. Alexander Bailey, 503 Cyber Protection Team, U.S. Army Cyber Protection Brigade

Gartner, Inc., a leader in information technology research, defines Threat Intelligence (TI) as: "evidence-based knowledge, including context, mechanisms, indicators, implications and actionable advice, about an existing or emerging menace or hazard to assets that can be used to inform decisions regarding the subject's response to that menace or hazard."

The process of generating TI can be correlated to the Army's Intelligence Preparation of the Battlefield (IPB) process, specifically step four – Determine threat/adversary courses of action (COA). In this step, Priority Intelligence Requirements (PIR), or indicators, are generated to inform a commander of an adversary's expected scheme of maneuver that ultimately allow him to select a friendly COA based on established decision points. PIRs are important because they trigger decisions that determine friendly maneuver. Similarly in the cyberspace domain, Indicators of Compromise (IOCs) if valid or associated with a high degree of confidence, are critically important because they should trigger decisions on how cyber mission forces (CMF) maneuver in cyberspace. Therefore, it is prudent for defenders to rapidly provision IOCs for the widest dissemination, as fast as possible, and in a common format that allows automated consumption by defenders and Defensive Cyberspace Operations (DCO) tools.

Indicators of Compromise are critically important because they should trigger decisions on how cyber mission forces maneuver in cyberspace.

A myriad of problems exist that currently prevent the rapid dissemination of IOC data including equities, need to know, classification, and others. The most notable impediment to date is the lack of a standard format for IOC data that contributes to the production of semi-structured/unstructured TI in the form of PowerPoint presentations, PDF documents, and Excel spreadsheets. This condition imposes a tremendous burden on Intelligence Analysts as they spend more time data wrangling than actually conducting intelligence analysis (correlation, predictive analysis, etc.). Fortunately, solutions to this problem exist that are mature and widely adopted by the federal government and civilian entities, particularly the Department Homeland Security (DHS). One such solution is Homeland Security's use of Structured Threat Information eXpression (STIX)[1] and its integration into the DHS Automated Indicator Sharing (AIS) system. AIS enables the exchange of cyber threat indicators between the Federal Government and the private sector at machine speed, and is a model that CMFs could use.

Cyber Guard (CG) is a joint training exercise focused on a "Whole of Nation" approach to defending against a domestic cyber-attack. Incident response teams from the DoD, federal government, and private industry participate in the event, providing a broad spectrum of experience, knowledge, and operational expertise. One of the primary training objectives is to conduct fast (near real-time) and reliable intelligence sharing. To that end, the DHS National Cybersecurity and Communications Integration Center (NCCIC) provides forensic and analytics support to the exercise to facilitate intelligence sharing. However, DHS does not produce STIX formatted intelligence products at the exercise. Cyber Guard would be an excellent opportunity to propagate the idea and value of using STIX at scale.

In practical terms the intelligence production workflow would begin with the creation of a STIX formatted report by the NCCIC or any CG participant. The document would then be disseminated to participants through established knowledge management mechanisms or via TAXII servers. Most teams use Security Onion as an Intrusion Detection System (IDS) which would allow for automated ingestion of STIX formatted intelligence into the BRO intelligence framework by leveraging the STIX common Python data model objects. As an example, accessing all IOCs and context within a STIX formatted report can be accomplished programmatically in less than 10 lines of Python code.

1 STIX is a language, not a program or system as might be implied

omise, and Structured Threat Information eXpression

The STIX repeatable python objects within the report contain attribute properties such as IP, File Name, Hash, etc.

IOCs do not equal intelligence, and their use must be part of a broader threat intelligence strategy that includes behavioral and pattern analysis. Sharing IOC data and ingesting it into IDS platforms would be a quick win and an automated process, thus reducing the current labor intensive work of Intelligence Analysts. The main barrier to overcome is the lack of standardization of threat intelligence products that are machine readable. STIX should be given serious consideration as a solution, and evaluated at joint training exercises like Cyber Guard. Whether STIX or another solution, the way ahead for addressing dynamic cyber adversaries requires improved mechanisms for disseminating and ingesting TI. Standardized TI shared at near real-time will enable the rapid and appropriate response from our cyber defenders.

Host analysts from 1st Cyber Protection Battalion conduct defensive cyberspace operations (DCO) at a critical facility in the Midwestern United States. Pictured: CW2 Joshua Neely and SSG Anthony Striano. (U.S. Army Photo)

CSCB (cont.)

Continued from page 6

The CSCB pilot program ended in May 2017. However, the Army has seen the way forward and continues to contribute forces to current and future National Training Center (NTC) rotations at Fort Irwin, California. The Signal Corps is moving forward with its plans to outfit all BCTs with trained cybersecurity soldiers and the Cyber Protection Brigade is developing ways to standardize network defense across the force. As more units are exposed to the benefits of cyberspace operations at the tactical level, the Army will continue to improve its information dominance capabilities and project power in and through cyberspace across the globe.

Members of the 1st Cyber Protection Battalion, the U.S. Army Corps of Engineers (USACE) Critical Infrastructure Cyber Security Center of Expertise (CICSCX), and Johns Hopkins University Applied Physics Lab (JHUAPL) collaborate to develop DAGGER dependency models for industrial control systems (ICS). (Photo by Maj. Joe Marty, 154 CPT, 1st Cyber Protection Battalion)

Continuation Page

Ever-Evolving CPB (cont.)

Continued from page 2

redesign, and requested 180 additional billets to enable the CPB's transformation to an operational maneuver brigade.

The additional personnel will fill newly authorized, mission-critical billets that are currently filled "out of hide" by personnel who will return to their rightful work roles on their respective CPTs. More than half of these newly authorized positions are designated for Department of the Army Civilians, who have proven invaluable to operations thus far. Here is a summary of the new C2 and enabling capabilities authorized under the recently approved manning document:

- 1st Cyber Protection Battalion (including Headquarters (HQ), A and B Companies)
- 2nd Cyber Protection Battalion (including HQ/A and B Companies)
- Cyber Fusion Center (CFC)
- Network Engineering, Research, and Development (NERD) Cell
- Cyber Readiness Inspection Activity (CRIA)
- Key Staff Elements (Unit Ministry Team (UMT), Brigade S6, S3 Cyber Division, etc.)

Wrapping up, it's clear to see that the Cyber Protection Brigade is an aggressive, innovative, future-focused organization that is, and will continue to be, well-postured *to defend the DOD's key terrain against specified threats, to deliver effects that ensure freedom of action in and through cyberspace, and to deny the same to our adversaries.*

Key Leaders from the 1st Cyber Protection Battalion learn about hydropower generation from a renowned Corps of Engineers hydropower expert. Pictured are: Chief Warrant Officer 3 Charles Frierson, Lt. Col. Aaron Gould, Maj. Joe Marty, and Maj. Justin Miller. (U.S. Army Photo)

CPB: Eager Lion (cont.)

Continued from page 4

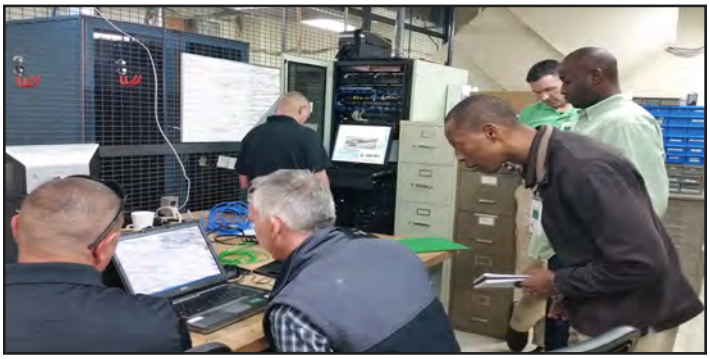
CJTF's ability to operate with degraded communications. To trigger the CERT, the inject team began running Low Orbit Ion Cannon (a well know DDoS tool). The CERT recognized this immediately, reported it, requested the appropriate IP blocks, and reported the denial of service (DoS) attack to the CJTF. Despite this warning, when the inject team began altering files, creating pop-ups, and closing programs, CJTF users failed to recognize and report the suspicious activity. After the inject team intensified the DoS efforts and eventually shut down systems, users finally began notifying the CERT, who identified the source and reported the activity.

A number of lessons learned were documented and shared at the conclusion of the exercise. The biggest takeaways were the inherent value of strong relationships with coalition partners; the phenomenal capabilities that CPTs bring to any operation or exercise; and we can ALWAYS count on well-intentioned computer users to keep the cyber defenders busy!

CPB Photo Page

Members of 2nd Cyber Protection Battalion pose with a partner Cyber Protection Team (Navy) while supporting a named operation at Joint Inter Agency Task Force - South in Key West, Florida. (U.S. Army Photo)

Personnel from the 1st Cyber Protection Battalion, the U.S. Army Corps of Engineers Critical Infrastructure Cyber Security Center of Expertise (CICSCX), and Army Cyber Operations Integration Center, pose for a photograph at the CICSCX national SCADA (supervisory control and data acquisition) lab in Branson, Missouri. (U.S. Army photo)



ICS/SCADA cybersecurity experts from 1st Cyber Protection Battalion conduct defensive cyberspace operations (DCO) at a critical facility on the east coast. Pictured: CW3 Kevin Pfanstiel, CW4 James Henry, SFC Fellom Alexander, SFC Brian Rowcotsky, and MSG Michael Bishop. (U.S. Army Photo)

Steel gray and black are the colors traditionally associated with Cyber units. The pale blue disc represents the globe itself and the worldwide reach of the organization through global networks. The gold compass rose exemplifies exploration of new technologies and how the Soldiers in the Brigade are pioneers in cyber defense. The 13 stars signify the 13 original teams in the organization. The black band around the globe and compass symbolizes the past, present, and future, and the white and gray shield allude to the organization's role as network defenders.

This is the end of the BYTE: Cyber Protection Brigade - turn the magazine over to read more!