

Volume 6, Issue 1

the BYTE

780th Military Intelligence Brigade

- * Expeditionary CEMA Teams
- * Brigade Holiday Ball 2017
- * Army Cyber Skills Challenge V
- * 2017 All-Army CyberStakes
- * Remembering Sgt. 1st Class Tommy Lee Robinson, Jr.



Everywhere and Always...



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, Army Civilians, 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 David (Dave) Branch
Commander

Command Sgt. Maj. James M. Krog
Command Sergeant Major

Steven Stover
Public Affairs Officer
and Editor



Columns

In every issue...

780 MI BDE CDR:	1
780 MI BDE CSM:	2
780 MI BDE: Photo Page	5
781st MI BN CDR:	7
782nd MI BN CDR:	8

CIVILIAN SERVICE:

• Serving the local community	9
• Down range, in the Work Center, at a Mission Site	13
• There is no "I" in team	14
INSERT: Soldier and NCO of the Year	27
780 MI BDE: Shoulder Sleeve Insignia	35
BDE Legal: Attorneys are also "Everywhere and Always..."	36
780 MI BDE: Military history of the "780th"	37
BDE SARC: SHARP: Everywhere and Always	39
BDE EOA: EEO applies to Army Civilians	40
BDE Chaplain: "Why do some people bounce and others break"	41
BDE Safety: Office ergonomics	41
Retention: A "Why I Stay...In the Fight!"	43
780 MI BDE: CSA and USCYBERCOM Vice CDR visit the Brigade	44

In Remembrance:

Sgt. 1st Class Tommy Robinson	56
--------------------------------------	-----------

the BYTE: INSCOM's nominee for the 2017 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.

Features

Soldier deploys with Red Cross to help others	15
2017 Best Warrior Competition: Cyber Soldier took up the gauntlet and enjoyed it!	29
2017 Brigade Holiday Ball	31
Army developing Expeditionary Cyber Teams to support tactical commanders	47
Cyber activities at the National Training Center supports real world operations	49
Expeditionary Cyber Support Detachment provides offensive cyber operations	51
Lightning Forge 18-01: Insights and lessons learned from integrating cyber into light infantry training	52

Articles

780th MI Brigade marks change in its “Keeper of the Colors”	3
CyCon U.S. 2017	6
AvengerCon II: Bigger and Better	10
B/781st: A requirement and what it will mean	11
D/781st: In the (defensive) fight	12
Cyber Soldiers conduct field training exercise to hone Warrior Skills	17
Hawaii Soldiers mentor local students in cybersecurity	19
Cyber Soldiers ‘lead’ from the front at Army Basic Leader Course	22
All-Army CyberStakes	23
Army Cyber Skills Challenge V	25
St. Isidore: Medals honor cyber professionals for excellence	34
The MD Chapter of Heroes on the Water	45

From the Editor

...And here I thought this issue would be my smallest; however, when the call went out for Army Civilian contributions -- this issue is officially the largest BYTE yet!

The theme for this issue is *“Everywhere and Always...”*

The 780th Military Intelligence Brigade is *“Everywhere and Always...In the Fight!”*

The Brigade is geographically dispersed throughout four states, 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).

In this issue are several articles written by and about our Army Civilians. As a team, our Soldiers, Civilians and contractors -- together -- we are *“Everywhere and Always...In the Fight!”*

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



On the Cover:

FORT IRWIN, Calif.

– Sgt. Camille Coffey (on the antenna), and Spc. Victorious Fuqua, both cyber operations specialists from the Expeditionary Cyber Support Detachment, 782nd Military Intelligence Battalion (Cyber), based out of Fort Gordon, Georgia, provide offensive cyber operations as part of the Cyber-Electromagnetic Activities (CEMA) Support to Corps and Below (CSCB) program at the National Training Center, January 18 through 24. (U.S. Army Photo)



“Everywhere and Always...”

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



What foresight from the builders of the 780th! Choosing a motto such as *Everywhere and Always* gave vision to what is now a reality for our unit.

What do I mean? Well, consider how

during the build phase of the Brigade, our focal points were simply the four geographic locations from which our teams trained and our headquarters elements developed processes and staff functions. Compare our build history to the tactical, operational, and strategic areas of our current focus, plus the continued home-based geographic presence and the deployed presence of 780th assets. My quick assessment tells me that we engage at some level of readiness, training and/or mission focus on 6 of the 7 continents! Reminds me of the Dr. Seuss book given often to graduates, *Oh, the Places You'll Go!*

As your commander, I am continually amazed at just how many missions and how much the 780th force is accomplishing. We are leading the Joint Force in readiness, in mission success, and in initiatives of the future. Internally to the Army, our senior leaders and battlefield units recognize our tangible contributions to the current fight and our potential impacts for future engagements! We are living our motto of *Everywhere and Always ...In the Fight*. As you read the articles and view the photos of this Byte edition, I hope you reach the same conclusion that I did – namely, that you all are making a difference in this warfighting domain!

As equally important, and more personal to me, is the knowledge that I've gained about what many of you are doing beyond our daily directed missions. Our Army has always prided itself on “**Mission First, People Always**” and we always will. My observations of the actions of our 780th Soldiers and Civilians expanded my understanding of the “people always” portion of this time-honored phrase. No doubt, our NCOs are

developing great Soldiers who are top performers at Professional Development Education schools; our Warrant Officers are leading technical efforts that inform the improvement of our teams, our training, and our development efforts; our Officers provide great focus to our teams and in many cases are performing beyond the traditional Team Leader position and influencing plans, policy and operations in a joint arena; our Civilian force is integrated into the NCO, Warrant and Officer team tasks while also leading many of our sustainable functions and hiring efforts to reach our manning goals for greater mission success. However, what has impressed me just as much is the numerous “off-duty” efforts of so many of you.

In our ranks, we have folks who serve Fort Meade Single Soldiers; coach and participate in base youth and unit sporting events; help Wounded Warriors and family members; contribute to community religious services and events; lead bike spin classes and run local farms; raise kids and grandkids; referee sports and volunteer as fire fighters; completed a career in uniform and now continue to serve; and teach computer skills to homeless Veterans. Wow!

Collectively, you, the Soldiers and Civilians of the 780th make me proud and keep me humble all at the same time. Thank you for truly being **EVERYWHERE AND ALWAYS.... IN THE FIGHT!**



Col. Dave Branch, commander, 780th Military Intelligence Brigade, gives a coin to Spc. Timothy Young for his help in supporting the Army Cyber Skills Challenge at Fort George G. Meade, Md., Nov. 16, 2017. (55th Signal Company photo)



...In the Fight!"

By Command Sgt. Major James Krog, senior enlisted leader, 780th Military Intelligence Brigade (Cyber)



The first six months in the position as your Brigade Command Sergeant Major have been a whirlwind.

In just this short time, I have visited the Soldiers and Civilians in Georgia, participated in a

training brief, talent management panel, a validation exercise, and other internal and external events; I have visited the Soldiers and Civilians in Hawaii, while observing an exercise that our CEMA (cyber-electromagnetic activities) Support to Corps and Below (CSCB) team participated in; I traveled to Texas to visit the Soldiers and Civilians there, while also visiting our Air Force counterparts in AFCYBER (U.S. Air Force Cyber Command); and I have traveled to Fort Irwin, California and watched our Soldiers professionally integrate with a Stryker Brigade Combat Team at the National Training Center.

At Fort Meade, we participated and fared very well in our DAIG (Department of the Army Inspector General) inspection; hosted numerous visitors, to include a Congressman, the Army Chief of Staff, and a multitude of other high ranking visitors. There was the annual Army Cyber Skills Challenge in November; and we executed a Leader's Week, and our annual Brigade Ball on Dec. 1.

We had a Soldier participate in the Best Warrior Competition at the Army level at Fort A.P. Hill, Virginia. We sent Soldiers and Civilians forward to support the Army's deployed forces. We continue to send Soldiers and Civilians to support our partners across the world. We have had multiple companies hold changes of command and responsibility. We also came through a safe and restful holiday season, while continuing to conduct operations.

This is all in addition to the normal daily activities across all our sites.

Throughout all of these events, I am constantly proud

of how the Brigade's personnel conduct themselves. I am grateful that the Army saw fit to place me in this position and look forward to our time together. It will be very busy, but it will also be rewarding.

The next quarter does not provide any relief. In fact, we will be busier than ever. It starts with some key leader visits, our semi-annual training briefs, a Brigade change of command, and our continued participation at the National Training Center. As this NTC rotation ended, the CSCB team immediately began preparing for Fort Bliss, Texas, and the next NTC rotation.

The Brigade will participate in language meetings, the 781st Military Intelligence (MI) Battalion will host a change of responsibility; two first sergeants will take responsibility of new companies; the deputy commanding officer and S3 (operations) will both change out; planning has begun for the next brigade-level Best Warrior Competition in April; and if all goes well, 781st MI Battalion will finish their move to the Deerpath facility.

This is just a small sampling of the events... Both JMOCs (Joint Mission Operations Center) at Forts Meade and Gordon will continue operations; all teams will continue performing their missions; and Soldiers and Civilians will train in and execute their assigned work roles. Meetings will be conducted and reports submitted. The Brigade will continue to be engaged in accomplishing its multitude of missions across the world.

I look forward to the task of ensuring this Brigade remains the best Brigade in the Army. You are all professionals who take pride in your duties and accomplishments and your accomplishments are many. Keep it up and the Brigade will continue on its path of excellence.

The motto of the Brigade is a true testament of what you do day in and day out. You are truly... **"EVERYWHERE AND ALWAYS.... IN THE FIGHT!"**





FORT GEORGE G. MEADE, Md. – Command Sgt. Maj. Sheldon Chandler (right), the outgoing senior enlisted Soldier for the 780th Military Intelligence (MI) Brigade (Cyber), relinquished his authority as the “Keeper of the Colors” to Col. Dave Branch, the 780th MI Brigade commander, during a Change of Responsibility ceremony on a field near the brigade headquarters, September 8. (U.S. Army Photo)

780th MI Brigade marks change

Story and photos by Steven Stover, public affairs

FORT GEORGE G. MEADE, Md. – The changing out of the 780th Military Intelligence Brigade’s senior enlisted Soldier is very significant event when you consider this is only the organizations sixth year in existence.

To a cyber unit and a branch still developing its culture, structure, identity and mission, the command sergeant major is a critical position to the success of the unit and its team members.

Command Sgt. Maj. Sheldon Chandler relinquished his position as the top enlisted member of the team to Command Sgt. Maj. James Krog in a Change of Responsibility ceremony on a grassy field next to the brigade’s headquarters, September 8.

In his remarks, Col. Dave Branch, commander of the 780th MI Brigade, said that the command sergeant major was the “Keeper of the Colors” – the flag toward which the unit Soldiers and Army Civilians rally around – a phrase that carries multiple meaning, as well as specified and implied duties.

“What it represents to me is a trust in our most senior enlisted member of the team; a reminder and ‘charge’ to set the environment through word and deed, to carry out the commander’s vision and to inform subordinate units and empower subordinate leaders to



FORT GEORGE G. MEADE, Md. – Soldiers of the 780th Military Intelligence Brigade (Cyber) render honors during the playing of the National Anthem during a Change of Responsibility ceremony whereby Command Sgt. Maj. Sheldon Chandler relinquished his authority as the “Keeper of the Colors” to Command Sgt. Maj. James Krog, on a field near the brigade headquarters, September 8. (U.S. Army Photo)

in its “Keeper of the Colors”

officer, 780th Military Intelligence Brigade (Cyber)

achieve mission success,” said Branch. “It also requires at the brigade level, especially a new evolving brigade such as 780th, to work laterally, and up and out to the larger communities in advancing understanding of the unit, its mission and the future possibilities that await.”

Branch compared the “Keeper of the Colors” expression to the brigade’s mission statement, which he also views as very broad and flexible.

“Unlike any other domain, the cyberspace domain in which 780th operates, is a shared domain where Services and Agencies work together with similar capabilities to achieve unified effects,” said Branch. “As the brigade mission statement reveals, we must gain and maintain freedom of maneuver in cyberspace and deny our adversaries the same.”

The brigade commander credited his outgoing command sergeant major for working with key personnel from U.S. Cyber Command, the Army Staff, Army Cyber Command, U.S. Army Intelligence and Security Command, the Cyber Center of Excellence, Fort Meade Garrison and fellow brigades across the Army, to further develop the Cyber culture, structure, identity, and mission within the Army and the Joint Environment.

“Over the last two years, it has been my absolute honor leading the Soldiers and Civilians of the 780th Military Intelligence Brigade,” said Chandler. “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.”

Although the brigade said farewell to its senior enlisted leader and his wife, Christina, an Army Family team that was also retiring after more than 25 years of active service to the Army and the Nation, the unit was welcoming back an Army Family team who was not new to the brigade.

After serving a tour of duty at the Cyber Center of Excellence, Command Sgt. Maj. Krog, and his wife Linda, return to the brigade after a previous assignment as the command sergeant major for the 782nd MI Battalion at Fort Gordon, Georgia; a subordinate command under the 780th MI Brigade.



FORT GEORGE G. MEADE, Md. – Command Sgt. Maj. James Krog (left), is the new senior enlisted Soldier for the 780th Military Intelligence (MI) Brigade (Cyber) and assumes responsibility as the “Keeper of the Colors” from Col. Dave Branch, the 780th MI Brigade commander, during a Change of Responsibility ceremony on a field near the brigade headquarters, September 8. (U.S. Army Photo)

“His vast experience and knowledge now gained from time in the Cyber Center of Excellence will move the brigade even further in operational success, evolution of culture, and advancement across the spectrum of missions,” said Branch.

Branch is extremely confident that Command Sgt. Major Krog will serve well as the newest brigade “Keeper of the Colors”, and live up to the brigade’s motto **“Everywhere and Always...In the Fight!”**





ODENTON, Md. – The 780th Military Intelligence Brigade (Cyber) said farewell to Lt. Col. Christopher Longo, the outgoing deputy commanding officer since May 2016, at a Hail and Farewell event hosted by the All American Steakhouse & Sports Theater. Lt. Col. Longo has been with the brigade since May 2011 and is going to a command within the Joint Cyber Operations Group. (U.S. Army Photo)



ODENTON, Md. – The 780th Military Intelligence Brigade (Cyber) said farewell to Command Sgt. Major (CSM) Cecil Reynolds, the outgoing senior enlisted leader for the 781st MI Battalion, at a Hail and Farewell event hosted by the All American Steakhouse & Sports Theater. CSM Reynolds' next assignment will be the position of command sergeant major for 1st Information Operations Command, Fort Belvoir, Virginia. (U.S. Army Photo)

"A master level expert..."



ODENTON, Md. – The 780th Military Intelligence Brigade (Cyber) said farewell to Command Sgt. Major (CSM) Jesse Potter, the outgoing brigade S3 (operations) sergeant major since July 2016, at a Hail and Farewell event hosted by the All American Steakhouse & Sports Theater. CSM Potter became the senior enlisted leader of the 781st MI Battalion in a Change of Responsibility ceremony, March 7. (U.S. Army Photo)



FORT GEORGE G. MEADE, Maryland – Chief Warrant Officer 5 (CW5) Thomas Bichard, 780th Military Intelligence Brigade was promoted to CW5 at a ceremony attended my fellow Soldiers, Family and friends, Dec. 14. CW5 is the fifth, and highest, warrant officer rank in the United States Army. They are master level experts of both the technical and tactical aspects of leading in their field. (U.S. Army Photo)

2017 International Conference on Cyber Conflict U.S.



WASHINGTON – Gen. Mark Milley, the 39th Chief of Staff of the U.S. Army, addresses the audience at the 2017 International Conference on Cyber Conflict U.S. (CyCon U.S.), Ronald Reagan Building, Nov. 7. As Milley was talking about the character of war and the fusion of technologies – how they are used, how they are applied, the doctrine, organizations, and training – he stated “And I would argue that we, the United States, we’re not going to get it right... what is important is that we get it less wrong than your enemy. In the moment of the conflict, that you have the innate ability to innovate and adapt faster than your opponent can. Those are great advantages inherent within American society, and American leadership, and American culture.”



WASHINGTON – Lt. Gen. Paul Nakasone, commanding general of U.S. Army Cyber Command, was the first keynote speaker at the 2017 CyCon U.S. and he talked about the influencers of future cyber conflict. The first point he discussed that was an influencer was people, because “at the end of the day it all does come back to people. One of things that we’ve learned over the past 12 to 18 months is the super-empowered individual...He is that 50x coder that I was talking about. He’s the person that has developed the ideas in terms of social media and how to get after ISIS in that space...that went out to academia...that went out to private industry, and said ‘here is what we need to do’ to get after an adversary in virtual space. That is the power of the super-empowered individual.”

780th MI Brigade Commanders Reading List



As your Commander, I am often asked, “Sir, what are your reading in your spare time?” Frankly, my readings are varied and sporadic in genres; I enjoy fiction, non-fiction, classics and Sci-Fi; I take recommendations from others openly.

For your amusement and/or attempt to gain insight in my thoughts, I gladly share here my readings over the last six months:

- Lord of the Flies
- Up and Vanished! (Podcast)
- Wooden
- The Immortal Life of Henrietta Lacks
- Shaken (Tim Tebow autobiography)
- Lilac Girls
- The Cyber Defense Review (Army Cyber Institute Quarterly)
- Something Rotten (Play)
- Serial (Podcast)
- Nearing Home



When faced with an 'either-or' decision, choose COA 3: 'and'

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



*"It's neither a pure starfish nor a pure spider." ~ Ori Brafman and Rod Beckstrom, **The Starfish and the Spider: The Unstoppable Power of Leaderless Organizations***

I have often stated in the past 18 months that the scope, scale, and complexity of our operations far exceed what is typically found in a traditional Army battalion. Although there are certainly larger battalions as measured by pure numbers of personnel, not many span five operational lines of effort, support no less than three operational headquarters, embed with numerous other Joint, Service, Interagency, and Industry partners, and conduct real-world operations 24/7/365, all without a force generation cycle familiar to most FORSCOM units.

And yet we also fill several gaps uncovered by the institutional arms of the cyber enterprise, routinely sending personnel to basic branch qualification courses (even teaching some of the courses ourselves) and accepting risk to on-going operations in order to spend time writing the qualification requirements and standards for our own work roles.

And although we have attained Full Operational Capability for all of our assigned Cyber Mission Force teams, we are still establishing new organizations such as the Cyber Solutions Development (CSD) detachment and a re-missioned company element, developing our own manning documents, creating our own force design, and seeking out our own operational opportunities (if not requirements) to employ the capability which we have generated.

The recent task organization of our teams into task forces only further accentuates the reality that we are continuing to evolve as a force, out-running our own headlights before the ink has dried on our doctrine. So as a force that proudly proclaims the unique pervasiveness of its operational domain, it is not just

important but absolutely imperative that we challenge our assumptions and embrace unorthodox methods of leading standard military hierarchies (i.e., spiders) while also recognizing that complete "flattening" (i.e., starfish) is likewise a non-starter in a warfighting organization accountable to the American people.

In instances such as this, when faced with the dilemma of opposing forces and competing requirements, we must choose the "and" option and create a new type of organization. As we have often acknowledged, **we exist in a hybrid operating environment, virtually deployed to an area of hostilities while physically stationed at a garrison installation.** Consequently, we must develop an unprecedented sustainable readiness model or we risk diminishing returns. It follows that this divergent reality also influences how we train, requiring leaders to carefully balance any impact to current missions while ensuring our readiness for future operations. We must reexamine our traditional training paradigms and consider how we measure, test, and report training readiness in the context of live environment training, while we also need operational commanders to acknowledge training requirements as a priority in their risk calculus.

In this ever-evolving environment, leaders must emphasize a set of clear guiding principles that reflect the Army's Values and serve as an azimuth for the centralized management and decentralized execution of operations in response to rapidly emerging requirements and dynamically changing conditions. As leaders, we must cope with flexible discomfort, admitting we do not have time to ask all of the right questions, let alone receive all of the answers. We must empower our subordinates to exercise disciplined initiative. We must accept an 'eyes on, hands off' leadership style. We must understand when to lead, when to follow, and when to move out of the way. And ultimately, we must realize that on future battlefields, it will be the Commander's intent that must be "everywhere and always" since physical and virtual network speeds will only increasingly outpace the human domain.

"Vanguard! When Others Cannot!"



“Everywhere and Always...”

By Lt. Col. Matthew Lennox, commander, 782nd Military Intelligence Battalion (Cyber)

In twenty years of service I have never been part of an organization that does so much every day. Keeping

pace with both training requirements and mission progress for each of the teams in Texas, Hawaii, Maryland, and Georgia is dizzying. Those missions have become our steady state operations. Members of the 782D are making additional contributions to the 780th Military Intelligence Brigade and Army Cyber Command. In the last 30 days, the Cyber Legion has had Soldiers in Australia, Japan, the United Kingdom, and Germany. In addition, the battalion has three Soldiers deployed to Afghanistan and Kuwait. We have Soldiers and Civilians attending professional schools and supporting exercises in Arizona, Pennsylvania, Florida, and Virginia.

Finally, the Expeditionary Cyber Support Detachment (ECSD) just returned from a 30-day rotation at the National Training Center (NTC) in California. They will soon be heading out to Fort Bliss, Texas to support another unit's training and then back to Death Valley to support another 30-day rotation at the NTC. The end result of all of this effort is that the Combat Mission Teams and Combat Support Teams are providing world class cyber support to the combatant commands it supports and helping to protect our service men and women in harm's way.

To sustain this tempo, the detachments, companies, and teams of the 782D need to continue to strengthen our “core,” the 8-10 people per team that truly drive operations, by refining our skill sets and building depth on our teams. This will become more important as we head into the summer PCS season.

As the turnover rate among our military members churns at about 35 percent per year, our civilian teammates will continue to be the subject matter experts for long term target continuity and experience. I do not expect this to change in the near future, and thank them for their professionalism and willingness to teach others. I would especially like to highlight the efforts of Sharon Martin, Kevin Ebersol, Matt Titus, and

Jacob Canard. Finally, welcome home to Lee Presto, an Army Civilian, returned in January from a yearlong deployment to Afghanistan.

While losing personnel to PCS (military moves) always hurts, the battalion will realize some benefit from the turnover of its uniformed members this summer. Chief Warrant Officer 3 (CW3) Kim Cooper, CW3 Candice Whitaker, and CW3 Tim Stevens, who each have more than three years of team experience, are moving over to Army Cyber Joint Force Headquarters. These moves will truly enable the JFHQ and our teams with a higher level of talent and experience at the staff level. These moves will provide soon-to-arrive Warrant Officers the opportunity to both learn from what we have done and bring new perspectives to the teams.

The totality of NCO experience is growing rapidly. This is particularly important to me as a former team lead. In many cases, the NCOs are assuming the old mantle of being the backbone of the force. During a recent visit by Col. Dave Branch, commander of the 780th MI Brigade and Command Sgt. Maj. James Krog, the brigade senior enlisted leader, each team highlighted their key NCOs. Many thanks to Staff Sgt. Blane Richoux (A Company), Sgt. Victoria Grizzard (B Co.), Staff Sgt. Timothy Stech (C Co.), Staff Sgt. Johanna Gutierrez (D Co.), Sgt. Christopher Cooper (E Co.), Sgt. Mitchell ‘Deadpool’ Godfrey (Headquarters & Headquarters Co.), Staff Sgt. Jason Lott (ECSD), Sgt. Genie Hoover (Detachment-Hawaii), and Sgt. Jose Acosta (Det.-Texas) for their superb performance over the last quarter.

Likewise, a number of Soldiers received high praise during the update to the brigade command team. In particular, Spc. Ryan Bruce (A Co.), Spc. Patrick Keller (B Co.), Spc. Joshua Beaumont (C Co.), Spc. Jesse Davis (D Co.), Spc. Brendan Heckman (E Co.), Spc. Justin Longshore (ECSD), Spc. Cyle Carlson (Det.-HI), and Spc. Alexis Lampkins (Det.-TX) stood out for their outstanding performance.

The Command Sergeant Major and I are truly humbled to be part of this great organization.

“Cyber Legion...Silent Victory!”



Serving the local community

By Capt. Leo Barajas, Battalion S1 (personnel), 781st Military Intelligence Battalion (Cyber)



Stanley McChrystal said in *Team of Teams: New Rules of Engagement for a Complex World*, “A leader’s words matter, but actions ultimately do more to reinforce or undermine the implementation of a team of teams.” An individual’s actions do speak loudly, and Ms. Kelli Cameron’s actions set a tone that carries across the workforce of the 781st Military Intelligence (MI) Battalion. As part of the 781st MI Battalion’s S1 (personnel) section, Ms. Cameron spirited example motivates others to think critically, generate productive feedback, mature and grow as a team, and as individuals in and outside of the workplace while helping others along the way.

Stanley McChrystal’s quote above characterizes the type of impact that Ms. Cameron, a senior human resource clerk, has within the 781st MI Battalion and on those she interacts with daily. Her extensive knowledge and dedication empowers personal and professional development of the battalion’s Soldiers and Civilians. Her belief is, for each Soldier and Civilian to learn, he or she must become actively engaged in the mission, goals, and objectives of the organization. Quietly, and with determined resolution, her leadership model is strengthening the

reputation of the battalion on and off post.

In her current capacity, Ms. Cameron works as an HR professional in the 781st MI Battalion’s (personnel) S1 section. She advises the leadership on all leave, finance and personnel strength matters. Ms. Cameron’s outstanding support within the Battalion has earned her the title “Ms. Dependable,” a title that she carries proudly. Other titles that she wears with honor and distinction include Retired Army Veteran and Active Civil Servant.

Ms. Cameron’s commitment to the Army values is illustrated at work, but also through the countless hours and attention that she volunteers on weekends and holidays giving back to those who are less fortunate. Ms. Cameron helps feed, clothe and provide for those in need within the Baltimore area as a volunteer with Happy Helpers for the Homeless. When asked about her volunteer work, she humbly responded, “People need help, and it is important to be active within your community. Don’t forget you also live here and their issues are your issues. If you were in that same situation, you would appreciate the help.”

The highly talented, professional workforce of the 780th MI Brigade consists of many outstanding Civilians exercising Servant Leadership, not seeking credit but expressing their values through their actions and serving as an example for others. Ms. Cameron is a leader through and through and we are honored that she is part of the team.





AvengerCon II: Bigger and Better

By 1st Lt. Samuel Sands, executive officer, Alpha Company, 781st Military Intelligence Battalion (Cyber)



FORT GEORGE G. MEADE, Md. – TOOOL instructors taught interested participants how to pick locks with varying stages of difficulty at Lockpick Village. (U.S. Army Photo by 1st Lt. Samuel Sands)

The second annual AvengerCon was held on November 15, 2017 at the McGill Training Center on Ft. George G. Meade, Maryland. Soldiers, Army Civilians, and civilians from industry in the surrounding area attended the conference.

AvengerCon's mission is to emulate a "hacker style" conference for the Army. The conference featured events such as keynote speakers, a Lockpick Village, Crypto Challenge, Hacker Trivia, Capture-the-Flag (CTF) competition, and a preview of the upcoming Army Cyber Skills Challenge V.

All ranks, military occupational specialties, and components (Active Duty, Civilian, Reservists, etcetera) were eligible to submit for the 'call for papers'. Throughout the event, 17 speakers presented their projects, research, stories, and thoughts.

Dr. Eugene Spafford, Executive Director Emeritus, Purdue University, gave a fantastic keynote about the history of cyber, the challenges of cyber as a force, and the value of lessons learned over the years. He stated that cyber needs to be far more encompassing than what the Cyber National Mission Force (CNMF) currently has scoped.

The presentations ranged from high level overviews of the CNMF and beginner level introductions of different topics to more advanced and technical talks about exploitation mitigation and payload patching.

Aside from listening to the presenters, participants were

free to roam around the venue and explore the other events.

The Lockpick Village was hosted by instructors from the local chapter of TOOOL, The Open Organisation of Lockpickers. Participants constantly stopped by to learn basic lockpicking skills and even attempt to pick a Master Lock. Some Soldiers ended up spending the entire day at this event and competed against each other in a series of lockpicking time trials.

The Crypto Challenge was put on by Staff Sgt. Ryan Moeller. This challenge introduced people to the world of cryptography by decrypting messages in various cyphers as well as using cracking secret codes with different techniques. Participants received raffle tickets for each challenge they successfully solved.

Spc. Thomas Grimes set up a CTF event from scratch where interested personnel attempted to hack their way through a digital obstacle course. In cybersecurity, a CTF is a cybersecurity competition usually designed to serve as an educational exercise to give participants experience in securing a machine, as well as conducting and reacting to the sort of attacks found in the real world.

1st Lt. Andreas Kellas organized the Hacker Trivia where participants gathered into teams to answer the most questions regarding various aspects of cybersecurity. This was a great way to bring participants together and socialize.

All in all, AvengerCon II was a great success. Plans for AvengerCon III are already underway!



FORT GEORGE G. MEADE, Md. – Participants hacking their way through last year's Army Cyber Skills Challenge. (U.S. Army Photo by 1st Lt. Samuel Sands)



Everywhere and Always... A requirement and what it will mean

By Capt. Rob Frost, commander, Bravo Company, 781st Military Intelligence Battalion (Cyber)



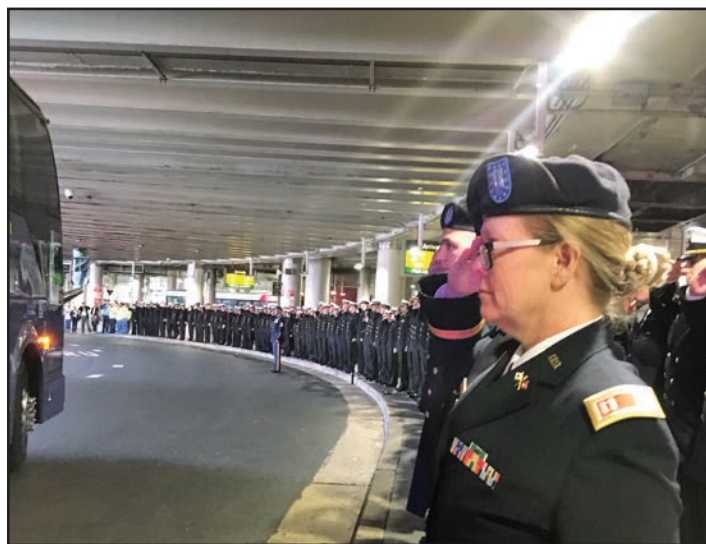
Lt. Gen. Paul Nakasone declared Fiscal Year 2018 “the Year of Delivery,” and the 780th Military Intelligence Brigade has surged across many LOEs (lines of effort) to create and produce tangible deliverables to drive the

force forward. Beginning last year but accelerating this year, Army Mission Teams have led the Cyber Mission Force on delivering on the promise that we would stand on our own and run our own operations. Whether as part of Joint Task Force-Ares, JFHQ-C (Joint Force Headquarters-Cyber) or the CNMF (Cyber National Mission Force), Army teams have poured sweat equity and talent into creating, staffing, and ultimately executing Title 10 Cyberspace Operations. We are moving closer to constant contact with a set of determined adversaries that have started from a position of advantage in this domain.

As Chief Warrant Officer 5 John O'Reilly likes to mention, two years ago we were not doing independent operations... at all. Teams relied on our partners to enable the intelligence gathering operations that we conducted, largely for our partners' benefit. We were Nowhere and Never. While this was a function of a junior force that was still being created, there was wide recognition that the paradigm had to change. Leaders with deployment experience understood that you can't sit idle behind static defenses in an irregular fight, but must push out and conduct reconnaissance. Leaders with technical experience understood that the nature of networks and automation enabled much more constant and aggressive campaigns than what we were conducting. Unity of effort from across the formation, from sub-element lead up to the BDE and JFHQ Commanders created irreversible momentum and now many teams are conducting regular operations on our own behalf. The trend must not stop. Teams should continue to push towards continuous operations in any network

that we choose, in order to operate in support of a commander's objectives. Doing so will break many processes and ways we do business. Staff sections will need to increase throughput. The art of making risk decisions, and who is making them, will need to be better understood. The capabilities required will dramatically increase in quantity and sophistication, likely driving an increase in resources committed to development, either in financial or technical capital. Analytic and reporting sections will have even more data to sort through, requiring better analysts and better trade craft. The demands of doing more operations and doing them more effectively will drive new changes, but will create a more lethal, effective force.

Constant contact, surveillance and reconnaissance are requirements if we want to be adequately postured to support our JFHQ and CNMF commanders. Pushing closer to truly being “Everywhere and Always ... in the Fight!” will drive change, but that push has inarguably already created positive change across the formation. Iterating rapidly and refusing to settle with the status quo is how we have started to learn to fight in our domain and contest adversary advantage.



BALTIMORE -- Soldiers from the 781st Military Intelligence Battalion participated in an Honor Flight on Nov. 4, in order to honor our American Veterans. There have been over a 190 flights this year and this weekend is the last for this season. (U.S. Army Photo)



Everywhere and Always ... In the (defensive) fight

By Capt. John Rollinson, commander, Delta Company, 781st Military Intelligence Battalion (Cyber)



Experts have widely accepted that defending a network is far more difficult than attacking or exploiting one. This observation is related to the fact that the offense maintains the initiative, choosing the specific time

and location of the attack, and the asymmetric aspect of an attacker needing only one of their attempts to succeed to breach a network. Conversely, network defenders have to be prepared to engage adversaries everywhere and always.

The requirement to be omnipresent and omniscient is difficult, if not impossible. In the past, local defenders, both government and civilian, maintained the idea that if they had antivirus software and a basic signature-based network intrusion detection system (NIDS) then they were secure. However, experience has shown that attackers can avoid triggering these signatures with ease, rendering the old paradigm obsolete and high-risk. Thus, today's cutting edge network defenses are moving toward anomaly and behavior-based detection of possible intrusions.

While these emerging techniques come with significant chances of fixing the inherent imbalance between offensive and defensive cyber operations, they come with three significant problems of their own: data storage, processing power, and inherent complexity. The first two problems are fairly straightforward; these techniques only work because they aggregate large amounts of data and perform calculations across the entire data set. The third problem, however, is often overlooked. Because of the machine learning or advanced mathematical algorithms used in identifying anomalies, it is often very difficult to understand exactly what makes an alerted activity anomalous. Without a clear understanding of how the algorithms work, defenders can quickly become overwhelmed and unable to separate false positives from actual attacks. In order

to adopt these new techniques, the Department of Defense (DoD) will have to solve this fundamental problem otherwise we will continue to place both Cyber Protection Teams and local defenders in information overload.

As network defense evolves, Delta Company, 781st MI BN, is presented with a unique opportunity to fundamentally shape how we defend the DoDIN (DoD Information Networks). Delta's unique location and partnerships enable the company to inform senior leaders about information gaps and to advise on the technical and policy solutions. These efforts will directly impact future DoDIN missions and help advance anomaly-based detection methods.

Moving forward, I believe we will continue to see National Cyber Protection Teams on the leading edge of defensive techniques for the DoD in the cyberspace domain. The key to this success will be in the ability to collaborate and scale these techniques into enterprise-wide solutions. In time, we may very well be perceived by our adversaries as having overcome the "impossible" and defensively be in the fight "Everywhere and Always."



FORT GEORGE G. MEADE, Md. – Soldiers from Headquarters & Headquarters Company, 780th Military Intelligence (MI) BDE and E Company, 782nd MI Battalion, fold the American flag at retreat on Feb. 20 -- a military custom that occurs at the post headquarters here daily at 5 p.m. Retreat is a tradition as old as the Army, and is a time when the flag is lowered and Americans render honors to the Colors of our Nation. (U.S. Army Photo)



Everywhere and Always... down range, in the work center, at a mission site

By Capt. Rob Frost, commander, Bravo Company, 781st Military Intelligence Battalion (Cyber)



We are all familiar with the great work that our Army Civilians do here in support of our missions, but recently a Bravo Company Civilian has been able to work all over the world. Ed Akers is a Target Digital

Network Analyst on 01 National Mission Team (01NMT) and has deployed to a mission site to help Cyber Protection Team (CPT) personnel, and, of course, brought his usual high impact abilities to the team during steady state operations.

First, Akers deployed with Combined Joint Task Force – Operation Inherent Resolve (CJTF-OIR) as an Unmanned Aerial System analyst and Cyber planner within the Cyber Electro-Magnetic Cell. While there, Akers worked with a variety of sections and units coordinating CJTF operations against unmanned aerial systems in theater. As a Subject Matter Expert from 01NMT, Ed represented an opportunity to fit a “best athlete” to an operational requirement for deployed forces. Akers brought a unique combination of innovation and initiative to the problem set for the Command and brought experience in target development and Signals Intelligence analysis. Ed was cited for his ability to leverage his analytic skills and the Intelligence Community’s immense capabilities in support of CJTF-OIR and subordinate units to help deliver operational effects throughout the Euphrates River Valley, Tal Afar and Raqqah. Returning from the deployment, Akers was able to share that operational perspective and understanding with the Soldiers he mentors within the Analysis and Production section.

Akers and another B Co. Civilian, Michael Suter, were first to jump into the breach when 01NMT was spun up in response to a crisis here in the states. After a suspected compromise occurred, with apparent ties to long running NMT interests, Akers and Suter traveled to the mission site to work side-

by-side with CPT responders. Working through the weekend, they provided a critical communication linkage from the defensive and incident response forces to the offensive forces working to support clearing actions. Their knowledge and understanding of the actor were described as “invaluable” by the team lead on the ground who noted that they brought a different view and perspective that would be challenging to replicate with just CPT personnel. The flexibility and desire to jump to a crisis enabled the NMT to rapidly understand a new mission set and begin posturing for follow on action.

Finally, and perhaps most importantly, Akers is an example of an expert mentor and trainer on 01NMT. Analysts of all experience and ability levels draw on his knowledge and utilize tools that he helped create and roll out for the team. While quick to correct people that “[he’s] a hacker and analyst not a developer,” his infectious enthusiasm and passion for the mission is a driving force behind many breakthroughs for the team. That combination helps Akers represent what the Army Civilian population brings that would be nigh impossible to replicate—experience, expertise and continuity to ensure the mission is always driven forward even as other personnel rotate.

Army Civilian Corps Creed

I am an Army civilian – a member of the Army team.

I am dedicated to our Army, our Soldiers and civilians.

I will always support the mission.

I provide stability and continuity during war and peace.

I support and defend the Constitution of the United States and consider it an honor to serve our nation and our Army.

I live the Army values of loyalty, duty, respect, selfless service, honor, integrity, and personal courage.

I am an Army civilian.



There is no “I” in team

By Betty Neilson, intelligence specialist, Bravo Company, 781st Military Intelligence Battalion (Cyber)



We are Army Civilians, members of the Army team; it is the first line of the Army Civilian Corps Creed. There is no “I” in team. We go where and when the mission requires.

Bravo Company’s civilians have deployed OCONUS to Iraq, Syria, Jordan, and UAE. In the past they have gone to the UK and Israel. Recently, some members have gone to the Pentagon to provide cyber expertise. They have routine engagements with Intelligence Community partners such as the FBI, CIA, NGA, and of course NSA. They also support short term requirements to the Cyber Center of Excellence, Fort Gordon, Georgia, to inform the development of cyber job qualification requirements. Bravo Company civilians support the Cyber National Mission Force’s Task Force-1, however, that does not prevent them from assisting other Task Forces when their mission needs exceed the available resources. During these times, the company’s Civilians and/or Soldiers are sent to support until the challenges are overcome and crises are averted. This affects our Civilians’ two-fold. The departing Civilian/Soldier quickly spins up on the new problem set and the remaining Civilians pick up the workload. The dedication to serve our Army, Soldiers, and other Civilians render this an opportunity to contribute – to bolster mission success. Bravo Company’s Civilians are heavy hitters; we possess the analytical mindset to perform malware analysis,

forensics, and extensive cyber related tradecraft. We are often contacted to advise and assist other teams/agencies. It is indeed for us, an honor to serve.

Across the 780th MI Brigade you will find a highly talented Civilian workforce with a wealth of experience; there are many retired military personnel with multiple deployments and others with unique and advanced skillsets. Such valued members of the Civilian corps fill the vital role of advisor and mentor in addition to normal work requirements. No amount of education or industry experience can replace what these Civilians bring to the fight. They are survivors of wars past and have strong backs. I have always believed strong backs make good bridges. Bridges that enable incoming warfighters to navigate safely across treacherous waters. These Civilians provide stability, continuity, and reach-back for those forward-deployed and a sanity check for those who remain.

Most Civilians could choose employment in the private sector for possibly higher pay, but they choose to serve rather than be served. Given the choice, I would much rather have a supervisor that was about service than one concerned about amassing a huge fortune for him or herself. Service provides a dignity and trust to work and human relationships that is absent in capitalistic endeavors. Perhaps, this is the litmus test for those considering Civilian service, being a member of the Army team – teamwork is imperative to go everywhere and be fit for the fight – remember, there is no “I” in team.

Service is the commonality and kinship of all Army Civilians. Whether deployed, providing reach-back, performing intelligence gathering/reporting, or Soldier support: we can be relied on by the Command; we don’t just recite Army values, we live them. We serve out of loyalty and duty to God and country; respect for leadership and command; we engage in selfless service, not for our own honor, but out of a belief of duty and respect to those we serve. We work not for reward, bonus, or personnel gain, but because we took the oath of service, to perform work with integrity and personnel courage, whatever the cost; to do the right thing. We are Army Civilians.





Soldier deploys with Red Cross to help others

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



FORT GEORGE G. MEADE, Md. – Sgt. 1st Class Rafael Ortiz, a cybersecurity noncommissioned officer with the 781st Military Intelligence Battalion, used his personal leave time to cover his 21-day deployment with the Red Cross to assist others after Hurricane Maria struck the Commonwealth of Puerto Rico, a U.S. territory, on Sept. 20. (Courtesy Photo)

FORT GEORGE G. MEADE, Md. – When Hurricane Maria struck the Commonwealth of Puerto Rico, a U.S. territory, on Sept. 20, it left a swath of destruction throughout the island and left an indelible impact on the entire population of more than 3.4 million American citizens.

For one Soldier, the opportunity to make a difference in the place he calls home was a calling he could not ignore.

Sgt. 1st Class Rafael Ortiz, a cybersecurity noncommissioned officer with the 781st Military Intelligence Battalion, and a newly minted Red Cross team leader, used his personal leave time to cover his 21-day deployment with the Red Cross to assist others during this humanitarian crisis.



NARANJITO, Puerto Rico – Sgt. 1st Class Rafael Ortiz is pictured here with family members from his hometown and his Red Cross team members while on a humanitarian mission, Oct. 15. (Courtesy Photo)

“My family – parents, grandmother, sister, uncles, aunts, etcetera – live in Puerto Rico. Immediately after the hurricane, a lot of people were doing fundraisers. I felt that I could be more useful by going myself as volunteer,” said Ortiz. “So, I sent a lot of applications to different organizations to become a volunteer to go to Puerto Rico. The Red Cross was the first one that responded to my application. I went through an interview process, then a deployment briefing, and finally I received my assignment.”



NARANJITO, Puerto Rico – Sgt. 1st Class Rafael Ortiz (left), a cybersecurity noncommissioned officer with the 781st Military Intelligence Battalion and a Red Cross team leader, works with a member of his team to provide assistance items to local residents in Ortiz's hometown during a humanitarian mission Oct. 15.

after hometown crisis



ADJUNTAS, Puerto Rico – Sgt. 1st Class Rafael Ortiz (kneeling center), a Soldier and a Red Cross team leader, poses with his team members and a family from the Adjuntas municipality at the family's home, Oct. 16. The family allowed the Red Cross team members to use their front yard to distribute assistance items and fixed their truck when it broke down. (Courtesy Photo)

When Ortiz first arrived in Puerto Rico on Oct. 13, his initial responsibility was reunification. His job was to assist the people outside the Commonwealth with reconnecting with their family members on Puerto Rico.

While an important job, Ortiz asked to be moved to a section called bulk distribution because he wanted to be close to the people.

“For 16 consecutive days, I was the team lead of a group that went out with a truck to distribute food, water, hand sanitizer, tarps, and other items to different municipalities,” said Ortiz. “We visited 13 municipalities (sometimes more than once).” Ortiz said while his Red Cross team had a direct impact on over 18,000 people, it still wasn’t enough – he wanted to do more.

“I saw a little bit of everything. I saw people with no power, water, food, jobs, home... I saw others in better conditions. (Today) most of the island is in bad shape, especially the inside of it. In the mountains, the situation is bad,” reflected Ortiz. “One of the things that I will never forget is when we ran out of items at the distribution site. I had to tell about 400 people that we didn’t have any more food, water, and etcetera. It broke my heart... It happened almost everywhere we went.

Some people left crying.”

Two memorable events Ortiz says have marked him for life were his visits to the municipalities of Utuado and Aguas Buenas.

“Utuado was the worst affected area. After I went there the first time I asked to be sent again,” said Ortiz. “The need in Utuado is big. During my third time there, people immediately knew who I was. They were so happy to see us back. The second memory is the visit to an orphanage in Aguas Buenas. We had some food and water left so I asked the local police if they knew of a place where what we had was needed. They took us to an orphanage and we left everything there. Those kids marked my life.”

Ortiz said, regardless of the ongoing humanitarian crisis, the people of Puerto Rico have a good attitude. “The people were smiling and thankful for the assistance,” said Ortiz. “They understand it will take hard work and a long time for things to get back to normal; however, they take one day at a time. The best way to describe the people there is with one word – resilient.”



COMERÍO, Puerto Rico – Sgt. 1st Class Rafael Ortiz, a cybersecurity noncommissioned officer with the 781st Military Intelligence Battalion and a Red Cross team leader, is shown working with a group of volunteers from Dubai to provide assistance items to local residents on Oct. 25. (Courtesy Photo)



Cyber Soldiers conduct field training exercise

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



GLEN ARM, Md. – Soldiers from E Company, 782nd Military Intelligence Battalion (Cyber), conducted a field training exercise to hone their knowledge of U.S. Army Warrior Tasks and Battle Drills, November 16 and 17. (U.S. Army Photo)

GLEN ARM, Md. – Mission first. It's a response Soldiers hear a lot; however, for one command team in the 780th Military Intelligence (MI) Brigade (Cyber), making the time to train their Soldiers on the U.S. Army Warrior Tasks and Battle Drill is also important. E Company, 782nd MI Battalion conducted Exercise Empire Strikes at Gunpowder Military Reservation, Maryland November 16 and 17 in order to ensure the Soldiers remained proficient in their Soldier skills. "We don't get a lot of the warrior culture in this unit – just by nature of our (cyber) mission," said 1st Sgt. Stanley Collins, senior enlisted leader for E Co., 782nd MI Battalion. "So making time to have the Soldiers go out there and do those basic Soldier things – carry their rifle, wear their gear, take instructions, move like a Soldier does...all those things are important." Collins also wants to ensure his Soldiers are trained and prepared for their next duty assignment. "We have Soldiers that are not 17-series (cyber operations) or 35Qs (cryptologic cyberspace intelligence collector/analyst), and these Soldiers are going to go back out to the force...this is their first duty station and the likelihood of them going to a tactical assignment after this is high," said Collins. "I don't want to send them to that next company and they don't know how to put their gear together."

According to 1st Lt. Bijesh Shrestha, a cyber officer with E Company, the event highlights were: a Leadership Reaction Course (LRC) for teambuilding and a leadership opportunity for the junior enlisted Soldiers; land navigation classroom training; and a field exercise focused on enabling the Soldiers to succeed at the noncommissioned officer (NCO) academy and other aspects of being a Soldier. The event culminated with a Squad Tactical Exercise (STX) that combined the training learned the previous day on various Warrior Tasks within a tactical scenario. Additionally, the unit linguists were tasked within the scenario to speak in Farsi with local nationals to ensure mission success. Staff Sgt. Brian Morelli, a platoon sergeant in E Company, and an STX cadre member, said the intent for the STX was to build the team.

"Getting the Soldiers to communicate in different ways. Getting them to interact in ways that isn't in the normal day-in and day-out not only helps build the team, but improves those interpersonal skills that we are going to be able to reap the benefits of later when we get back into the office," said Morelli.

Morelli and Collins also wanted to ensure the training was meaningful.

"Everybody complains in the field. It's not that you complain, but what you're complaining about," said Morelli. "They should be complaining that it's cold,



GLEN ARM, Md. – Soldiers from E Company, 782nd Military Intelligence Battalion (Cyber), conducted a field training exercise to hone their knowledge of U.S. Army Warrior Tasks and Battle Drills, November 16 and 17. (U.S. Army Photo)

to hone their Warrior Skills



GLEN ARM, Md. – Soldiers from E Company, 782nd Military Intelligence (MI) Battalion (Cyber), conducted a field training exercise to hone their knowledge of U.S. Army Warrior Tasks and Battle Drills, November 16 and 17. (U.S. Army Photo)

they should be complaining that it's early, complaining that they're tired... What they shouldn't be complaining about is the quality of the training and I didn't hear complaining out of anybody. Everybody enjoyed themselves."

Throughout the training, each Soldier rotated into a leadership position to prepare them for future Non-commissioned Officer Education System (NCOES) courses and their subsequent assignments as Army leaders.

"I definitely appreciated the STX and I hope that we continue to do it, because I enjoy learning," said Sgt. Justin Riopelle, a cybersecurity specialist with E Company. "I also realize that being a squad leader is a difficult job... running around like a chicken, making sure everyone has 100 percent accountability, the equipment is ready to go, what they need – it's a very difficult job and I appreciate the people who are squad leaders... it was definitely a learning experience. It helps with the leadership role. It helps you manage your time and

build that self-confidence."

For one Soldier, using her linguist skills during the STX showed her the importance her skillset can have on the battlefield.

"I definitely learned a lot. It was a good refresher and being a linguist, the only one in the squad, I was the only one who could translate during the mission," said Spc. Andrea Medina, a cryptologic linguist with E Company. "I realized how much pressure was put on me because of it. It made me realize how much impact being a linguist can have on a squad."

Medina also understands the importance of the training.

"In addition to this being about mission readiness – we are in a cyber unit – a lot of us are at our desks all day, but some of us, like myself, I am a linguist, I'm MI. I can go to a FORSCOM (U.S. Army Forces Command) unit," said Medina. "I'm not going to stay cyber forever, so it was nice to do those Soldier things again. The camaraderie was awesome... and it was a nice teambuilding experience."

Collins said the command already has plans for the next field training exercise and will host these events on a regular basis.

"The biggest challenge we have is the availability of the Soldiers," said Collins. "Because they do have a live mission that they're doing."



GLEN ARM, Md. – Soldiers from E Company, 782nd Military Intelligence (MI) Battalion (Cyber), conducted a field training exercise to hone their knowledge of U.S. Army Warrior Tasks and Battle Drills, November 16 and 17. (U.S. Army Photo)



Hawaii Soldiers mentor local students in

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



WAHIAWA, Hawaii – Soldiers from Detachment Hawaii, 782nd Military Intelligence Battalion, based out of Schofield Barracks, Hawaii, teach cybersecurity to Junior Reserve Officer's Training Corps cadets from Leilehua High School as part of a nationwide CyberPatriot program, Nov. 20. (U.S. Army Photo)

WAHIAWA, Hawaii – Gen. Mark Milley, the 39th Chief of Staff of the U.S. Army, recently mentioned it would be up to the next generation to figure out how to successfully fight and win the Nation's future conflicts.

"For those of you who are in the military who are 25 years old or younger...you're going to have to lead the way. People my age do not have the answers."

Soldiers from Detachment Hawaii, 782nd Military Intelligence (MI) Battalion, based out of Schofield Barracks, Hawaii, are teaching cybersecurity skills to Junior Reserve Officer's Training Corps (JROTC) cadets from Leilehua High School as part of the nationwide CyberPatriot program.

According to the team's coach, retired Army Lt. Col. Nick Spiridigliozzi, the Leilehua High School JROTC senior instructor, "CyberPatriot is the premier high school cyber defense competition in the Nation. It teaches students how to secure computers' networks

and all the things associated with it."

Last year the Leilehua High School CyberPatriot team made it all the way to the CyberPatriot IX National Finals in Baltimore, Maryland; however, Spiridigliozzi views the CyberPatriot program as more than a competition – he says the program is vital to our national security.

"We don't have enough people in cybersecurity right now and these kids we're training are going to protect this nation," said Spiridigliozzi. "Also, it gives these kids a career, a vocation,

and if they go in that direction, it gives them a lot of knowledge in cyber defense. I feel very strongly that even though I'm retired I'm still contributing to national defense by training these kids...at least bringing in the right people to train them."



WAHIAWA, Hawaii – Spc. Evan Wittman, Detachment Hawaii, teaches basic networking to Leilehua High School JROTC cadets (left to right) Kayla Orr, Jacob Huerta, and Alex Ruiz-Zamora, Nov. 20. (U.S. Army Photo)



WAHLAWA, Hawaii – Chief Warrant Officer 3 Lee Unrein, Detachment Hawaii, teaches Windows operating system basics and security to Leilehua High School JROTC students Daniel Brink (right) and Nicholas Lipka. (U.S. Army Photo)

Detachment Hawaii has been mentoring the Leilehua High School JROTC CyberPatriot team since the 2015-2016 school year and the coach and students attribute their success to the Soldiers.

“As far as I’m concerned, they are the best mentors in the nation. They are extremely knowledgeable, motivated, they have so much initiative and they think out of the box,” said Spiridigliozzi. “That means great training for the students, and without the Detachment there really is not a successful CyberPatriot program here. It all boils down to the mentors. Great kids, but if you don’t have great mentors teaching these students they are only going to go so far, and the 782nd will take these kids as far as they want to go.”

Cadet Tyler McWilliams is a 10th-grader at Leilehua High School and a second year CyberPatriot team member. For McWilliams, CyberPatriot has shown him cybersecurity is what he plans on studying in college.

“CyberPatriot is a way for me to get accepted into colleges. Also, it looks good on resumes,” said McWilliams. “Plus it’s a lot of fun with the people you get to meet and hang out with.”

Spc. Evan Wittman, from Detachment Hawaii, is the lead CyberPatriot mentor for the Leilehua Mules (the school’s official mascot). Wittman volunteers because he wishes he had this opportunity when he was in high school and he really enjoys the program.

“I really enjoy coming in – the kids are excited to learn, the kids are here for a reason,” said Wittman. “They’re not here to waste time. They enjoy what they do and it gives me a sense of purpose for where I am in my career right now.”

Wittman said they teach cybersecurity from the ground level and build their way up.

“We start with the initial foundational information – basic networking, basic protocols, port assignments – what looks right on a system,” said Wittman. “We teach them that baseline and then we move forward into more in-depth topics of networking. We spring into VLANs (Virtual Local Area Networks), we go into different types of routing protocols, OSPF (Open Shortest Path First), later on we’ll do BGP (Border Gateway Protocol), Windows and UNIX. We start showing them how to identify threats on their system, so different types of malware, either very basic script kiddie malware, or something a little bit more advanced.”

(Continued on the next page)



WAHLAWA, Hawaii – Spc. Jacob Cochran (standing right), Detachment Hawaii, teaches Leilehua High School JROTC cadets (left to right) McCain Compton, Christian Villarreal, and Tyler McWilliams, about the Linux operating system, Nov. 20.. (U.S. Army Photo)



WAHIAWA, Hawaii – Sgt. Kevin Kang, Detachment Hawaii, 782nd Military Intelligence (MI) Battalion, based out of Schofield Barracks, talks to Leilehua High School JROTC cadet Tyler McWilliams about the Linux operating system, Nov. 20. (U.S. Army Photo)

(Continued from the previous page)

Sgt. Kevin Kang, another CyberPatriot mentor from Detachment Hawaii, discussed how the scoring system works.

“The competition, and the CyberPatriot team, is split up into three main categories – Windows, Linux and networking,” said Kang. “In networking, they are tasked build a model. The cadets are given the specifications of what the network should be doing and they use a Cisco packet tracer to select the devices and create the connections that will create a functioning network. For Linux and Windows the objectives are similar. The cadets are told there are some unauthorized user accounts, or they need to shut down a service, or there is some malicious software on the computer – find it and get rid of it. Once they do those then there is an automatic scoring system, it plays a sound affect, and those points show up on a webpage.”

Spiridigliozzi said the team completed the first round of the CyberPatriot competition earlier this month.

“For rounds one and two we’re trying to score as high

as we possibly can to make sure we’re in the Platinum tier which allows us to be eligible for the national finals,” said Spiridigliozzi. “Round three is the state finals, and of course from there we want to be the first place team in the state within our tier. After that is the regional round and the regional round allows you to go to the finals.”

This year’s competition is expected to be even harder and Kang mentioned the students are solving problems that even their mentors have to “dig in and look ourselves.”

However, at the end of the day the coach and mentors agree that what they’re doing is more than a competition – CyberPatriot is cybersecurity...and it’s important to national security.

Editor’s Note: The CyberPatriot team from Leilehua is returning to the CyberPatriot X National Finals in April 2018 for the fourth time in the past seven years,



SCHOFIELD BARRACKS, Hawaii – Sgt. Jennifer Currey, Detachment Hawaii, reenlisted for an additional six years of continued service while on a U.S. Army Chinook helicopter, December 14. Joining her in the skies above Hawaii, were Currey’s husband, Sgt. Zachry Currey, and her command team. Nov. 20. (U.S. Army Photo)



Cyber Soldiers 'lead' from the front at Army Basic Leader Course

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



FORT INDIANTOWN GAP, Pa. – Soldiers from the 780th Military Intelligence (MI) Brigade (Cyber) completed the Army Basic Leader Course and two of them received honors at a graduation ceremony on Sep. 27.

The brigade's graduates were: Spc. Devin Aikens, C Company, 781st MI Battalion (Cyber); Spc.

Victoria Grizzard, B Company, 782nd MI Battalion (Cyber); and Spc. Jeremiah Will, Headquarters and Headquarters Company, 781st MI Battalion (Cyber).

The Army's Basic Leader Course is a branch-immaterial course that provides basic leadership training to allow Soldiers in the grade of Pfc. through Staff Sgt. the opportunity to acquire the leader skills, knowledge and experience needed to lead team and squad size units. The month-long course is part of the Noncommissioned Officer Professional Development System and is taught Army-wide.

According to Will, who made the BLC Commandant's List, BLC graduates have the ability to perform the duties of an Army sergeant and should be able to confidently accomplish those duties "to and above the prescribed standard."

"The toughest part of the course was maintaining the high degree of performance necessary to earn a place on Commandant's List," said Will. "My advice for Soldiers preparing for BLC is to speak with those who have recently gone in order to understand what is expected and get a head start on preparing for the task ahead."

To make the Commandant's List, students must earn an average GPA of 90 percent or higher, receive no adverse counseling statements, earn a first-time passing rating on all graded criteria and achieve a superior rating in three of the four demonstrated abilities (written communication, oral communication, leadership skills, or contribution to group work).

Aiken recommended Soldiers know the NCO Creed and the Army Song, hone their land navigation skills, and maintain their military bearing.

"Most importantly – stay positive," said Aiken. "The toughest part for me was working with other Soldiers who had different views, beliefs, cultures, and levels of military bearing."

Grizzard was also on the Commandant's List and received the Distinguished Leader Award.

The Distinguished Leader Award is used to recognize the student who demonstrates the highest leadership ability out of the entire BLC class. To be considered, the students must earn a place on the Commandant's List and receive above a 90 percentile average in both garrison and tactical leadership evaluations.

"After meeting these requirements, myself and the other candidates competed at the Leadership Board which tested our knowledge on all topics covered during the course," said Grizzard. "A high focus was also placed on recitation of the Creed of the Non-Commissioned Officer. I was chosen as the winner for the Leadership Board and was then awarded the Distinguished Leader Award."

Soldiers from the 780th MI Brigade attend the BLC taught by the 3rd NCO Academy, 166th Regiment, Pennsylvania Army National Guard, at Fort Indiantown Gap.



FORT INDIANTOWN GAP, Pa. -- The BLC graduates are shown above with their leadership and a family member following the ceremony (left to right): Sgt. Maj. Jesse Potter, the Brigade S3 (operations) sergeant major; Spc. Jeremiah Will, Headquarters and Headquarters Company, 781st MI Battalion (Cyber); Will's mother, Rosie-Linda Will; Spc. Devin Aikens, C Company, 781st MI Battalion (Cyber); Spc. Victoria Grizzard, B Company, 782nd MI Battalion (Cyber); and Command Sgt. Maj. Cecil Reynolds, the senior enlisted Soldier for the 781st MI Battalion (Cyber). (U.S. Army Photo)



Brigade Soldiers excel in cyber competition

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



WASHINGTON -- 1st Lt. Christian Sharpsten (center), a software developer assigned to the 781st Military Intelligence (MI) Battalion, 780th MI Brigade (Cyber), had the highest score in the officer category and placed first overall in the All-Army CyberStakes competition and received a certificate from Lt. Gen. Paul Nakasone, commanding general of U.S. Army Cyber Command (ARCYBER), at an award presentation at the 2017 International Conference on Cyber Conflict U.S. (CyCon U.S.), Ronald Reagan Building, Nov. 7. (U.S. Army Photo)

"More generally, the focus areas that CTF competitions tend to measure are vulnerability discovery, exploit creation, toolkit creation, and operational tradecraft," said Bundt. "Success in CTF competitions demands that participants be an expert in at least one and ideally all of these areas."

In this year's event, 602 participants registered and 499 of them solved at least one challenge. The number of participants included more than 200 from the CNMF.

"The variety of challenges requires deep knowledge of multiple computer architectures, file and file system formats, encryption schemes and learning new protocols and specifications on the fly," said Bundt.

2nd Lt. Edward Woodruff, a capability developer assigned to the 781st MI Battalion, 780th MI Brigade, said cyber challenges are a hobby of his. Woodruff, who had the third highest score in the officer category and placed third overall, prepared for the event by doing reverse engineering and binary exploitation (BE) in his free time.

Woodruff competes in these type of events because he sincerely enjoys them. Also, he was beaten by 1st

WASHINGTON – Soldiers from U.S. Army Cyber Command's 780th Military Intelligence (MI) Brigade (Cyber) and the Cyber Protection Brigade harvested both individual and unit honors in the All-Army CyberStakes (AACS) award presentation at the 2017 International Conference on Cyber Conflict U.S. (CyCon U.S.), Ronald Reagan Building, Nov. 7.

Hosted by the Army Cyber Institute (ACI), the AACS competition is an annual Online Capture-the-Flag (CTF) competition open to anyone in the U.S. Army plus the four Service Academies and ROTC cadets. This year's event ran from Sep. 30 through Oct. 9, and featured a significant newcomer to the competition – Soldiers assigned to Cyber National Mission Force.

Like many other CTF events, there are five basic categories of challenges: Binary Exploitation, Reverse Engineering, Forensics, Cryptography, and Web Exploitation. According to Lt. Col. Josh Bundt, an instructor of digital forensics and research scientist with the Army Cyber Institute, United States Military Academy, the challenge categories provide hint into the skill sets required for CTF challenges.



WASHINGTON -- Gen. Mark Milley (center), the 39th Chief of Staff of U.S. Army Cyber Command, and Lt. Gen. Robert Caslen, Jr. (right), to audience members who are cadets, lieutenants and captains associated with Nov. 7. (U.S. Army Photo)

Lt. Christian Sharpsten, a software developer assigned to the 781st MI Battalion last year and was hoping to pass him this time. Alas, in this good-natured competition, Sharpsten not only bested him, but was this year's overall AACS winner.

"Maybe next year," hopes Woodruff. "Capture the flag events, such as CyberStakes, realistically emulate the battlefield of cyberspace and act as an effective training tool for those looking to do development type work."

The first place finisher in the enlisted category was Spc. Thomas Dignan, also with the 781st MI Battalion. When the event started Dignan had just finished Joint Cyber Analysis Course (JCAC) and then phase II of the Army's 17C (Cyber) training at the Army Cyber School, Ft Gordon, Georgia.

"Programming and tinkering have been my hobbies for a long time," said Dignan. "I regularly spend time to sharpen my skills through personal projects."

Dignan believes cyber challenges like AACS is an opportunity for those Soldiers "willing to take the initiative to learn new skills" and "separates those who want to excel."

For those Soldiers or Army Civilians looking to compete and win in CTF competitions, Bundt credits the Trail of Bits CTF Field Guide @ <https://trailofbits.github.io/ctf/>, and refers those interested in 'winning' CTF competitions to the Trail of Bits site.



WASHINGTON -- Spc. Thomas Dignan, a recent U.S. Army Cyber School graduate and now assigned to the Headquarters and Headquarters Company, 781st MI Battalion, 780th MI Brigade (Cyber), had the highest score in the enlisted category in the All-Army CyberStakes competition and received a certificate from Lt. Gen. Nakasone, commanding general of ARCYBER, at an award presentation at the 2017 International Conference on CyCon U.S., Nov. 7. (U.S. Army Photo)

The 2017 All-Army CyberStakes Winners:

Officer Category:

- 1st Lt. Christian Sharpsten, 780th MI Brigade (1st overall)
- 2nd Lt. Matthew Shockley, Cyber School (2nd overall)
- 2nd Lt. Edward Woodruff, 780th MI Brigade (3rd overall)

Warrant Officer Category:

- Chief Warrant Officer 3 Phillip Smith, Cyber Protection Brigade
- Chief Warrant Officer 2 Benjamin Koontz, Defense Information Systems Agency
- Chief Warrant Officer 2 Nicholas Kleck, 1st Information Operations Command

Noncommissioned Officer Category:

- Sgt. Matthew Cundari, Cyber Protection Brigade
- Sgt. 1st Class Zachary McElroy, Cyber Protection Brigade
- Sgt. Andrew Canino, 476th Chemical Battalion, U.S. Army Reserve

Junior Enlisted Category:

- Spc. Thomas Dignan, 780th MI Brigade
- Spc. Stephen Cosolito, 780th MI Brigade
- Spc. Blaine Milburn, Cyber Protection Brigade

Total Score by Unit:

- 780th MI Brigade
- Cyber National Mission Force
- Cyber School



of the U.S. Army, Lt. Gen. Paul Nakasone (left), commanding general of the 59th Superintendent of the U.S. Military Academy, stand with the cyber force, at the 2017 International Conference on CyCon U.S.,



Army Cyber competition pushes competitors

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



FORT GEORGE G. MEADE, Md. – Spc. Andrew Doering, 741st Military Intelligence (MI) Battalion, completes different tasks and solves problems during the capture the flag portion of the Army Cyber Skills Challenge V competition, Nov. 16. (U.S. Army Photo by Spc. S Nicholas Maloney)

FORT GEORGE G. MEADE, Md. – The warrant officers of the 780th Military Intelligence (MI) Brigade hosted the 5th Annual Army Cyber Skills Challenge (ACSC) to determine this year's champion, 14 to 17 November 2017.

According to event organizers, this was the first year the competition was held at three different geographic locations: Fort Gordon, Georgia; Fort Meade, Maryland; and Schofield Barracks, Hawaii.

Chief Warrant Officer 4 Kirk Bond, a cyber operations technician, and an event coordinator and cadre member, said the event was created with the intention of challenging participants, both physically and mentally, to crown the individual with the highest composite score as the ACSC Champion.

"We want an overall winner who is a good technical guy and who can still physically go out there and bring it," said Bond.

The physical events included a modified Army Physical Fitness Test, a modified Army Combat Readiness Test, and a ruck march with a thirty-five pound rucksack. The technical portion lasted a full 24-hours and included programming, exploitation, forensics, and a crypto-analysis challenge.

The ACSC was introduced in 2013 as a means for the warrant officers to provide a training opportunity for Soldiers and Civilians in the Brigade. Since its inception in 2013, the event has grown from 11 participants to more than 60 this year. The event continues to be designed and executed by warrant officers in the 780th Military Intelligence Brigade; however, officers and non-commissioned officers have volunteered to help build events and serve as cadre.

"The people who are doing this event are doing it because it's something that they are passionate about," said Bond. "There's a good portion of people that are here to test their skills and a smaller portion are here just to see if they have what it takes."

The ACSC V overall champion was 1st Lt. Andreas Kellas, Cyber Solutions Detachment (CSD), 781st MI Battalion. Kellas not only enjoys Capture the Flag (CTF) competitions, but enjoys fitness events as well.

"I just feel fortunate to have an opportunity to spend two days at work on my favorite hobbies," said Kellas.

The technical champion for this year's event was 1st Lt. William Brattain, CSD, 781st MI Battalion. He strongly recommends cyber Soldiers and Civilians participate in the ACSC, especially those assigned to the brigade, because "the competition is what our mission focus is supposed to be."



FORT GEORGE G. MEADE, Md. – Soldiers with the 704th Military Intelligence (MI) Brigade and 780th MI Brigade, compete during the jug squatting event for the Army Cyber Skill Challenge V competition, Nov 15. (U.S. Army photo by Pfc. Joseph Cannon)

physically and mentally



FORT GEORGE G. MEADE, Md. – Spc. Thomas Dignan, 781st Military Intelligence Battalion, buddy man carries 1st. Sgt. Michael Wahl during the Army Cyber Skill Challenge V competition, Nov. 15. (U.S. Army photo by Spc. Dra'corius White)

“I (have been) competing in similar competitions over the past six to seven years,” said Brattain. “I was on a dedicated hacking team in college and we would do CTF style competitions just about monthly. Much of my training came from off-duty CTFs, personal projects, as well as general education.”

For this year’s runner up, Spc. Thomas Dignan, C Company, 781st MI Battalion, the competition provides “a great opportunity to get out of the office and push competitors both physically and mentally.”

Dignan also participated in the Army Cyber Institutes’s All-Army CyberStakes competition in October and said that event prepared him for ACSC. For hardware he brought his personal Macbook Air and noise canceling headphones. He said he only needed basic software, such as VMware to run the Windows and Linux VMs (virtual machines), vim



FORT GEORGE G. MEADE, Md. – Chief Warrant Officer 2 Joseph Dixon, 780th Military Intelligence Brigade, grades the PT test portion of the Army Cyber Skills Challenge V, Nov. 15. (U.S. Army photo by Sgt. Zachary Burke)

(Virtual Infrastructure Management) and xxd (a Linux command) to edit text and binary files, and unix command line tools to do everything else.

“If you want to be successful at CTFs, get good at programming and working on the command line,” said Dignan. “After that, look into developing specific skills for the different CTF categories i.e. reverse engineering, web exploitation, forensics, etcetera, a good resource for that is: <https://www.trailofbits.com/>. (Also) participate in as many CTFs as you can. Interested Soldiers can go to <https://hackcenter.com/> and sign up for the All-Army CyberStakes 2017 to do practice problems.”

Col Dave Branch, commander, 780th MI Brigade, and Chief Warrant Officer 5 John O’Reilly, the brigade’s senior technical advisor, recognized the individual and overall winners at an award ceremony in the brigade annex on Fort Meade, and organizers skyped in competitors from Georgia and Hawaii. The ACSC champions for 2017 are –

- ACSC V champion – 1st Lt. Andreas Kellas, Cyber Solutions Detachment (CSD), 781st MI Battalion;
- ACSC V runner up – Spc. Thomas Dignan, C Company, 781st MI Battalion;
- Technical champion – 1st Lt. Will Brattain, CSD, 781st MI Battalion; and
- The Iron Warrior – Spc. Alfredo Santos, 782nd MI Battalion, Georgia.



FORT GEORGE G. MEADE, Maryland – 1st Lt. Will Brattain, Cyber Solutions Development Detachment (CSD), 781st Military Intelligence (MI) Battalion, Spc. Thomas Dignan, C Company, 781st MI, and 1st. Lt. Andreas Kellas, CSD, are all presented awards for placing in the Army Cyber Skills Challenge V by Col. Dave Branch, commander, 780th Military Intelligence (MI) Brigade, Nov. 17. (U.S. Army Photo by Spc. S Nicholas Maloney)



780th Military Intelligence Brigade

LOYALTY ▣ DUTY ▣ RESPECT ▣ SELFLESS SERVICE ▣ HONOR ▣ INTEGRITY ▣ PERSONAL COURAGE

NCO of the Year

SSG Humberto Gutierrez
HHC, 780th MI BDE





By: (name, rank, unit)

780th Military Intelligence Brigade

LOYALTY □ DUTY □ RESPECT □ SELFLESS SERVICE □ HONOR □ INTEGRITY □ PERSONAL COURAGE

Soldier of the Year

SPC Johnny Long
Detachment Hawaii
782d MI BN





Cyber Soldier took up the gauntlet and enjoyed it!

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

Merriam-Webster defines taking up the gauntlet as someone who is “willing and ready to fight, argue, or compete with someone or to do something that is difficult but necessary: to accept or respond to a challenge.”

Sgt. Johnny Long of Mesquite, Texas, assigned to Detachment Hawaii, 782nd Military Intelligence (MI) Battalion, 780th MI Brigade, was that someone who accepted the challenge to be the Army’s Best Warrior. He began a ten month journey from his selection as the detachment representative, through the battalion, brigade, North Region U.S. Army Intelligence & Security Command (INSCOM), INSCOM, and U.S. Army Cyber Command competitions, and culminated with his participation at the U.S. Army-level Best Warrior Competition in October.

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 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.

Although Long did not win at the Army-level, it was a significant accomplishment to beat out the best of the best through each level of competition, and this spring units throughout the Army will be looking for the next Soldier and noncommissioned officer to pick up the gauntlet.

However, what does it take to get there?



#2 KNOW THE ARMY WARRIOR TASKS

FORT BELVOIR, Va. – “I would recommend the best warrior competition to others,” said Sgt. Johnny Long, Detachment Hawaii (DET HI), 782nd Military Intelligence Battalion. “It’s a unique experience, it was fun, definitely going to learn some things out here, like when they did the warrior tasks that nobody expected. It’s a broadening experience.”



#3 12-MILE RUCK WITH A STRESS SHOOT EXERCISE

GLEN ARM, Md. – “Ultimately, there is going to be one Soldier and one noncommissioned officer selected to move forward,” said Sgt. Major Craig Hood, the operations sergeant major for the 704th Military Intelligence Brigade. “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.”



1 EXPECT THE UNEXPECTED

FORT GORDON, Ga. – “The Jared is an operational fitness challenge; it’s a CrossFit event,” said Sgt. 1st Class Ian Sabin, 782nd Military Intelligence (MI) Battalion, noncommissioned officer in charge of the 780th MI Brigade’s Best Warrior Competition. “The actual event itself is 70 push-ups...the push-ups are going all the way down, releasing your hands so your chest is hitting the ground, and then pushing back up. It’s also 40 Army PRT (physical readiness training) rowers. That’s one rotation. You have to do four rotations to complete the regime, followed by pushing and pulling a 200 pound sled, within a one-hour time limit.”



#4 TIMED OBSTACLE COURSE
GLEN ARM, Md. – “All the competitors came here with the same goal in mind,” said Sgt. Johnny Long, DET HI, 782nd MI Battalion. “We went all out, but for fun, pushing each other. It’s been a crucible experience.”



#8 BOARDS AND ESSAYS
FORT BELVOIR, Va. – “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 Command Sgt. Maj. William Bruns, the senior enlisted leader for U.S. Army Cyber Command. “These Soldiers are really, really exceptional.”



#5 WARRIOR TASKS DURING THE RUCK MARCHES
FORT A.P. HILL, Va. – “These competitions are never easy,” said 1st Sgt. Peter Novak, Headquarters and Headquarters Company, U.S. Intelligence & Security Command. “But with this year’s iteration of Best Warrior, we really wanted to push the op-tempo and see how the Soldiers would respond.”



#9 THE ARMY-LEVEL COMPETITION IS INTENSE
FORT A.P. HILL, Va. – “I know that parts of it have been rougher than I expected, parts that were more fun than I expected,” said Sgt. Johnny Long, DET HI, 782nd MI Battalion. “But there have also been a lot of opportunities for experiences that I wouldn’t otherwise have had.”



#6 MULTIPLE COMBATIVE ENGAGEMENTS
FORT A.P. HILL, Va. – “It’s been great so far. It’s been rough, exhausting, it’s been extremely challenging, a little miserable and I think that’s the point at this level,” said Sgt. Johnny Long, DET HI, 782nd MI Battalion.



#7 THERE WILL BE AN ARMY PHYSICAL FITNESS TEST
FORT BELVOIR, Va. – “The Army established the Best Warrior Competition to identify the best warrior,” said Sgt. Maj. Jesse Potter, operations sergeant major for the 780th Military Intelligence Brigade. “You’re not going to be the NCO of the year, or Soldier of the year, you’re going to be the best warrior for the Army.”



#10 THE LEONIDAS -- BRIGADE BEST WARRIORS
FORT MEADE, Md. – Command Sgt. Major James Krog, the brigade senior enlisted leader, Staff Sgt. Humberto Gutierrez, brigade NCO of the Year, Sgt. Johnny Long, brigade Soldier of the Year, and Col. Dave Branch, brigade commander.



BALTIMORE – Soldiers, Army Civilians, contractors and their Family members of the 780th Military Intelligence (MI) Brigade (Cyber) started the festive season by getting together for a formal occasion at their annual Holiday Ball at the Westin Baltimore Washington Airport hotel on Dec. 1.



#1 The 780th MI Brigade Holiday Ball began with a gift exchange.



#2 Guests were greeted by cheerful volunteers.



#3 The receiving line for the Holiday Ball included the brigade senior enlisted advisor, Command Sgt. Maj. James Krog, the brigade commander, Col. Dave Branch, the keynote speaker, Rear Adm. T.J. White, commander, Cyber National Mission Force, and their spouses.





#4 Each of the guests were welcomed to the Holiday Ball by the receiving line.



#7 Following the 'toasts'; the guests honored our missing and fallen comrades.



#5 The Holiday Ball began with the posting of the Colors, an invocation and a stirring rendition of our National Anthem.



#8 There were games – musical chairs, with a 'scavenger hunt' twist – an event won by Command Sgt. Maj. Bart Larango, the senior enlisted advisor for the 782nd Military Intelligence Battalion...



#6 There was a cake cutting to recognize the youngest Soldier.



#9 ...and the 'Twelve Days of Christmas' whereby gifts were presented to lucky guests, including movie tickets

780th
Military Intelligence
Brigade
Holiday Ball
December 1, 2017



#12 After the colors were retired...



#10 The keynote remarks were provided by Rear Adm. T.J. White, commander, Cyber National Mission Force. He talked about the work of the Cyber Soldiers that fell under his operational command, the burden they share, and addressed the Family members present when he stated "your Soldiers...they do it for you."



#13 ...there was dancing!



#11 Rear Adm. White even presented a gift to our brigade commander -- complete with a "Go Navy! Beat Army!" label. Fortunately...the Admiral was wrong and Army beat Navy 14-13!



#14 All in all...a very festive and fun event.



Medals honor cyber professionals for excellence

By U.S. Army Cyber Command



FORT BELVOIR, Va. – Thirty-five military and civilian cyber professionals have been honored this year with the St. Isidore Army Cyber Award for 2017.

The award, sponsored by the Armed Forces Communications-Electronics Association (AFCEA), recognizes “individuals who demonstrate exceptional initiative, leadership, insight, and cyber excellence within their area of expertise,” according to nomination criteria on AFCEA’s website.

There are three levels of the annual award – gold, silver and bronze medals presented based on categories of recipients and levels of achievement.

The award was created in 2011 after St. Isidore of Seville (560-636) was chosen to “represent the highest ideal of the essence of cyber security and the study of the evolving world of challenges of tomorrow.” The saint is considered by many to be the patron of the Internet, though Pope John Paul II never made a final decision on his official selection. A scholar who coined the word etymology – the study of origins – his publication of a 20-volume series of books on a wide range of topics earned the saint the title of “father of the encyclopedia.”

Although considered an Army award, an Air Force member was among the recipients this year for the first time. Maj. James Crawford of the 24th Air Force’s 67th Cyberspace Operations Group earned a medal for his service as deputy chief of operations for Joint Task Force Ares. The task force, which provides unified, sustained cyberspace support to counter-ISIL efforts in Iraq and Syria, is within the purview of Army Cyber Command, making its personnel, who come from all branches of service, are eligible for the Saint Isidore Award.

The brigade commander Col. Dave Branch and the senior enlisted leader, Command Sgt. Major James Krog, presented several of the medals during the December 1 Holiday Ball.

The brigade’s 2017 recipients are:

SILVER:

- Maj. Michael Arner
- Maj. Scott Bobier
- Master Sgt. Matthew Varney
- Leonard Lewis

BRONZE:

- Chief Warrant Officer 3 Jason Hurst
- Sgt. Maj. Jesse Potter
- Sgt. 1st Class Thaddeus Watson
- Larry Williamson





Shoulder Sleeve Insignia

The Institute of Heraldry, U.S. Army Center of Military History



Description

On a shield shaped embroidered item, the upper corners arched inwardly, edged with a 1/8 inch (.32 cm) Yellow border, blazoned as follows: Sable, a depiction of a flowing grid Argent, charged with a disc throughout per pale Celeste (Oriental Blue) and Argent (Silver Gray) fimbriated Or, bearing a lightning bolt of the second and an arrow of the first, point upward in saltire, surmounted by a key erect, ward to sinister of the fifth, all above an arc of five mullets of the second. The overall dimensions are 3 1/4 inches (8.26 cm) in height by 2 3/4 inches (6.99 cm) in width.

Symbolism

Oriental blue and silver gray are the colors traditionally associated with Military Intelligence units. The flowing grid signifies the Brigade's link to the U.S. Cyber Command and Army Cyber Command. The modified disc suggests the unit's responsibility to provide pervasive, comprehensive, intelligence information and analysis. The combination of the shield vertically and the divided background of the disc alludes to the continuous intelligence missions and the day and night protection of cyberspace, reflecting the unit's motto "Everywhere and Always...In The Fight." The arrow symbolizes readiness; the lightning bolt denotes swiftness and the key conveys security of knowledge and truth. The five stars represent the unit's support for the Joint Forces.

Background

The distinctive unit insignia was approved on November 6, 2013.

FORT GEORGE G. MEADE, Md.

-- On December 1, 2011, the 780th Military Intelligence Brigade (Cyber) officially unfurled its colors for the first time during an activation ceremony at Fort George G. Meade, Maryland; however, it wasn't until April 23, 2014, the Soldiers of the 780th MI Brigade, transferred from wearing the U.S. Army Intelligence and Security Command (INSCOM) patch to wearing their own unique shoulder sleeve insignia. (U.S. Army Photo)





Attorneys are also “Everywhere and Always...In the Fight...”

By Frank Colon, cyber operations attorney, 780th Military Intelligence Brigade (Cyber)



*The author in Iraq
(Courtesy Photo)*

While the U.S. Army Judge Advocates General Corp is 243 years old, my prior service, the U.S. Navy, waited 197 years before implementing the Navy JAG Corps in 1967. Regardless,

since our introduction, attorneys have been part of the fight.

Military Attorneys serve in three primary roles: Representational, (trial and defense counsel, and legal assistance): Administrative, (contracts, ethics, and support to installation commanders): and Operational. In the first two, Judge Advocates and civilian attorneys provide support to the war fighters by ensuring fair and proper justice and legal advice to service members and leadership. Operational attorneys do much more than support the warfighter, they in many cases, the accompany the warfighter to the fight.

With the ever increasing complexity of warfighting, operational attorneys ensure that everyone from the commander to the pointy tip of the spear, understand the legal parameters of the mission, rules of engagement, applicable international treaties, and the parameters of coalition partners participation. We also settle claims for wrongful damages and ensure battlefield contractors deliver.

In my career, I have deployed to sea aboard the USS Ronald Reagan, to Afghanistan, and several SEAL Team missions that were so narrowly authorized that a Judge Advocate was required to accompany the Team and provide in-theater operational legal advice.

Maj. Steve Janko has been deployed to Afghanistan, Iraq, and Kosovo for a total of five deployments over his career. Similarly, he too provided instant on-the-spot legal advice in the battlespace, to commanders and troops, to ensure the mission was conducted in accordance with the law,

while ensuring the rules of engagement supported the warfighter.

Operational attorneys are seamlessly integrated into the battle rhythm, working with intelligence analyst and operational planners to legally get to “yes.” The presence of attorneys in the fight has ensured the vast majority of our operations are lawful and stand up against scrutiny. In the rare occasion when an operation was flawed, the records collected by the attorney prior to the approval clearly demonstrated no intent to violate the law of war by any of the operational participants. Attorney participation in the fight has ensured that all of our branches, under the most violent and dangerous conditions, conduct warfare in a manner that fosters public respect and admiration for our missions 24/7/365.

We deploy accurate and timely violence in a lawful manner that ensures minimal casualties and maximum effect. This lethality could not be deployed in a lawful manner without the presence of operational attorneys in the battlespace. Together, we are all *“Everywhere and Always in the Fight!”*



FORT GEORGE G. MEADE, Md. – Maj. Gen. Christopher Ballard (right), commanding general, U.S. Army Intelligence and Security Command (INSCOM), runs with Col. Dave Branch, commander of the 780th Military Intelligence Brigade (Cyber) and the Cyber brigade Soldiers during the Fort Meade Joint Service Resilience and Remembrance Run September 8. (U.S. Army Photo)



The Military History of the “780th” – A distinguished record

Maj. Steven Janko, Brigade Judge Advocate, 780th Military Intelligence Brigade (Cyber)

What’s in a name? The answer may surprise you. The history of the “780th” numerical unit designation encompasses far more than cyber warfare in the 21st Century. In fact, it includes amphibious tank warfare in the Pacific, B-24 Liberator bombing runs in Europe, fighting with Patton’s Third Army in France and Germany, providing military police support in Northern Ireland, building oil pipelines in Burma to support combat operations, lobbing artillery rounds against North Koreans, and even performing ordnance support on the home front. U.S. Army units receive their numerical designations in a variety of ways.

The unit numerical designation of 780th has been utilized several times in U.S. Army History. During World War II, the 780th Amphibious Tank Battalion participated in combat operations in Leyte and Okinawa during the Pacific Campaign against Japan.



780th Amphibious Tank Battalion fought in the Pacific during World War II

In the European Theater, the U.S. Army Air Force 465th Bombardment Group was composed of three Squadrons: the 780th Bombardment Squadron, the 781st Bombardment Squadron and the 782nd Bombardment Squadron. These three Army Air Force Squadrons operated B-24 Liberators from Pantanella, Italy. It is interesting to note that these three Bombardment squadron unit designation numbers happen to match the current Battalion numerical designation of the 780th Military Intelligence (MI) Brigade and its two respective battalions: 781st MI Battalion at Fort Meade, Maryland and the 782nd MI Battalion headquartered at Fort Gordon, Georgia with operational detachments in Hawaii and Texas.



The 465th Bombardment Group during World War II was composed of the 780th, 781st and the 782nd Bombardment Squadrons.

Also serving in the European Theater during World War II was the 780th Ordnance Light Maintenance Company, which was part of the 80th Infantry Division. The unit landed in Northern France on August 2, 1944 and began combat operations just six days later on August 8, 1944 under Patton’s Third Army, fighting in both France and Germany. The Division returned to the United States in January 1946 after supporting peace keeping operations in war-torn Europe. In 1952, the 780th Ordnance Company was reorganized as Virginia-based Reserve unit in the 80th Division.

Also in the European Theater, the 780th Military Police Battalion provided law enforcement support in Northern Ireland during World War II under Headquarters, United States Army Northern Ireland Force (USANIF)



The 780th EN Company battled malaria, dysentery and typhus while constructing pipelines.

of service which includes more than cyber warfare

In the Asian Theater, the 780th Engineer Petroleum Distribution Company was activated on August 14, 1943 at Camp Claiborne, Louisiana and operated in Burma and China, during World War II. It was one of several engineering units involved in building the longest military pipeline from India to China in order to provide much needed oil to friendly forces.



The 780th EN Company battled malaria, dysentery and typhus while constructing pipelines.

The 780th Field Artillery Battalion was an Army Reserve battalion headquartered in Roanoke, Virginia. During the Korean War, the 780th Field Artillery Battalion engaged in combat operations in Korea from April 1951 to December 1954 while attached to X Corps, Eighth US Army.



780th MI BDE personnel currently support worldwide combat operations

This brings us to the 21st Century. Some U.S. Army units receive their numerical designations methodically, such as brigades with a parent division (e.g., 1st Armored Brigade Combat Team, 1st Infantry Division or 1-1 ABCT). In other cases, units receive more random numerical designations when established, e.g., separate brigades which operate

independently of a parent division, such as the 780th Military Intelligence (MI) Brigade.

The U.S. Army approved the establishment of an Army Cyber Brigade and designated it the 780th MI Brigade, effective October 1, 2011. It is interesting to note some of the important differences between the 780th MI Brigade and previous units with the 780th unit designation. First, our cyber brigade is the first brigade-size element which has the 780th numerical unit designation. Previous 780th units were only company-, battalion- or squadron-sized elements. Second, previous 780th units were confined to conducting their operations in specific geographic areas of operations whereas -- the 780th MI Brigade currently supports worldwide combat operations. Third, previous 780th units were exclusively composed of uniformed personnel; however, the challenges of the 21st Century are more complex and require a more diverse fighting force to be successful. The current composition of the 780th MI Brigade therefore includes Active Duty service members, mobilized National Guardsmen and Reservists, Army Civilians and contractors.

The current diversity of the 780th MI Brigade is its true strength and a force multiplier when engaging in support to worldwide combat operations. Many of our civilians have extensive operational and technical experience obtained through service in the military, the federal government and in the private sector. This diversity enables the 780th to tackle a host of complex and dynamic challenges which arise on a daily basis and thereby keeps us "Everywhere and Always ... In the Fight."

Sources:

- *US Army Center of Military History at <https://history.army.mil>*
- *Corps of Engineers Units-CBI History at www.cbi-history.com/part_iv_eng.html*
- *Fuel for Freedom- the ABC Pipeline at www.cbi-theater.com/fuel*
- *80th Infantry Division at 80thdivision.com*



SHARP: Everywhere and Always!

By Kimberly Henne, Sexual Assault Response Coordinator, 780th Military Intelligence Brigade (Cyber)



The Army's Sexual Harassment/Assault Response and Prevention (SHARP) Program was created to assist in the prevention of sexual

harassment and sexual assault among our ranks of enlisted, officers and Army Civilians. We cannot do it alone. It takes each and every Soldier and Army Civilian to make it happen. The SHARP Program also provides a strong response with trained personnel, should an incident occur.

Sexual harassment and sexual assault violate our Army Ethics. Every DA Civilian and Soldier should expect to be treated with dignity and respect, and should give dignity and respect in return. Sexual harassment and sexual assault amongst our ranks destroys trust and directly impacts readiness and cohesion. Even one incident is one too many. It takes a serious toll on victims and their units; disrupts good order and discipline; and damages the reputation of the Army.

The SHARP Program's prevention efforts for sexual harassment and sexual assault reach across the Army. Within the 780th Military Intelligence (MI) Brigade, no matter where you are stationed or your temporary duty location, the SHARP Program is there to help you.

At our Brigade headquarters and within the 781st MI Battalion located at Fort Meade, we have 14 trained, D-SAACP (DOD Sexual Assault Advocate Certification Program) certified collateral duty victim advocates, with four more in training this spring. Our full-time SHARP team is also located at Fort Meade. Sgt. 1st Class Abraham Morales recently joined the SHARP Team as the full-time Brigade Victim Advocate (VA). He has been with the 780th MI Brigade for five years and has held a variety of positions. I have been with this unit for three years as the full-time Sexual Assault Response Coordinator.

In Georgia, we have eight collateral duty victim advocates with two more who will be in training this spring. We also have the full support of the SHARP Resource Center on Fort Gordon and the 116th MI Brigade and Cyber Protection Brigade. The SHARP

Resource Center helps track any cases we have in the area, provides continuing education to our collateral duty victim advocates, and provides response should our VAs not be available or a victim would prefer to chat with someone outside our unit.

In Texas, we have one Soldier trained and awaiting D-SAACP certification. He should be certified in February and we should have another Soldier in training this spring. We also have the full support of the 470th MI Brigade SHARP Team to assist should anyone wish to speak with someone outside our unit.

In Hawaii, we currently have two D-SAACP certified collateral duty victim advocates, and one who is trained and should be certified in February. We also have two more collateral duty Victim Advocates PCSing to Detachment Hawaii this spring from two other locations. On Hawaii, we have the full support of the Installation SHARP Resource Center and the 500th MI Brigade to both support our victim advocates in their continuing education, as well as support our Soldiers and DA Civilians should they need assistance from anyone outside our unit.

While traveling (TDY), my government phone is always available to you 24/7. Should you need to call, that number is (410) 693-4638. Sgt. 1st Class Morales also has a 24/7 telephone number, (410) 693-2937. Additionally, the DOD Safe Helpline is available at (877) 995-5247. They have a companion app for your phone and website. Any of these three resources can connect you with a counselor 24/7 and can help you find a SARC anywhere in the world at any time. The DOD Safe Helpline website also has an anonymous, monitored chatroom where survivors can chat with each other and the room is monitored by a certified counselor if needed.

So, as our unit is "Everywhere and Always... In the Fight," the SHARP Program and your SHARP Team are also "Everywhere and Always... In the Fight" to support all Soldiers and DA Civilians alike.



Equal Employment Opportunities applies to Army Civilians

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



Civilians play a vital role in the success of every day operations within the 780th Military Intelligence Brigade, and across the Army. Just like Soldiers, they are afforded protections within the workplace from

discrimination and unfair treatment. The Army's six categories of protections for Soldiers that include race, color, religion, sex (gender), national origin, and sexual orientation also apply to the Civilian workforce under the DoD Equal Employment Opportunity program. Civilians are also protected from discrimination based on disability, genetic information, and age.

The EEO program is governed by laws dating back to 1963 with the Equal Pay Act, rather than the UCMJ (Uniform Code of Military Justice). It works much differently from the Army's EO system. Civilian employees with a complaint have 45 days to file the complaint with an EEO representative, who will then conduct an inquiry and attempt to resolve the issue at the lowest possible level. This will include interviews, and mediation or counseling, known as

Alternate Dispute Resolution. If a resolution is not reached, the complainant will be notified of their right to file a formal complaint within 15 days. A formal complaint is allotted up to 180 days for an investigation to be completed. This is much longer and more drawn out than the 15 day timeline the Army uses for its EO complaint cases.

Civilians are also required to complete the EEO Anti-Harassment & No Fear Act training within the first 90 days of employment, and once every 2 years. This training can be found on www.lms.army.mil by searching the word fear. Civilians should also receive unit EO/EEO training on their unit's specific EEO policy and programs when mission permits, and are also encouraged to attend EO observances at their installations.

For more information, or if you have specific EEO questions, you can reach out to the Fort Meade EEO office at 301-677-6298/6295, or to the Fort Gordon EEO rep at 762-206-3500.

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





“Why do some people bounce and others break?”

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



We all receive junk mail daily, both in our email inbox and in our physical mailbox. Several weeks ago, just before the holidays, I received a brochure in my mailbox from a company specializing in resilient

furniture: simple, sturdy, water resistant tables and chairs (their words, not mine). Not fancy in any way, but built to last. They were not cheap either; a “no thrills” plain white folding chair was on sale for the unbelievable price of \$89.99, but wait, if you act now...no just kidding. They were not as pretty as the office chairs one would purchase at your typical office bargain store, but those chairs, as I am reminded every time I have to replace one, do not have a long life-span. They are pretty, but they don’t last.

There’s something to be said for basic, unadorned resiliency: the ability to get through, get over, and thrive after a fight, trauma, trials and tribulations. In this sense, sturdy beats stylish every time. A few years ago, USA today did a cover story on the subject of resiliency, asking the question, “Why do some people bounce and others break?” I use that article in my Marriage Resiliency Training. The article noted how some people who experience trauma or adversity withdraw into a shell, while others facing the same crisis not only bounce back, but bounce back stronger than ever before. It talked about how resiliency is being studied in universities, taught in corporate seminars, and in the military. Resiliency, the article said, could become the most important skill of the 21st century.

So, this leads me to ask the question, why do some people break down while others bounce back? Unlike furniture, I don’t think it has to do with our design. A chair can only be as strong as it was made to be; it can’t decide to be more resilient or less resilient. We, on the other hand, have access to support beyond ourselves. Our “design”, our emotional make-up resulting from parental and societal influences, can be overcome. A person who is, by nature, weak and easily discouraged does not have to stay that way.

There’s a verse in Philippians that is so often quoted,

its meaning is sometimes overlooked. Paul is talking about being able to face hard times as well as good times, and he states confidently, “I can do everything through Him who gives me strength.” (Philippians 4:13)

Resilience often comes down to a decision: whose strength will I draw from, my own, or God’s? The promise in God’s Word is, if you will look to God for strength, He will give it to you. All you have to do is ask...simple! I close with another powerful verse found in the Old Testament, “I lift up my eyes to the hills, where does my help come from? My help comes from the Lord, the Maker of heaven and earth.” (Psalm 121:1-2)

Office ergonomics

Computer related injuries are increasing with the use of computer technology in the workplace. Long and repetitive work at your computer workstation can create discomfort, muscle aches, and be the cause of work related injuries. If you sit behind a desk for hours at a time, you’re not doomed to a career of neck and back pain or sore wrists and fingers. Proper office ergonomics -- including correct chair height, adequate equipment spacing and good desk posture -- can help you and your joints stay comfortable at work.

The basic idea behind ergonomics is the try and keep the body in a neutral position and not to remain in the same position for too long. To understand the best way to set up a computer workstation, it is helpful to understand the concept of neutral body positioning. This is a comfortable working posture in which your joints are naturally aligned. Working with the body in a neutral position reduces stress and strain on the muscles, tendons, and skeletal system and reduces your risk of developing a musculoskeletal disorder (MSD).

MSDs are injuries or pain in the musculoskeletal system, including the joints, ligaments, muscles, nerves, tendons and structures that support limbs, neck and back. MSDs

(Continued on the next page)



Office ergonomics

By George Lawler, Safety Specialist, 780th Military Intelligence Brigade (Cyber)

(Continued from previous page)

can arise from a sudden exertion, or they can arise from making the same motions repeatedly, repetitive strain, or from repeated exposure to force, vibration, or awkward posture. Exposure to these known risk factors for MSDs increases a worker's risk of injury. MSDs can affect many parts of the body including the back, shoulders, neck and extremities.

MSD Signs and Symptoms. Users at risk for MSDs associated with computer use may experience some of the following signs or symptoms: Numbness or a burning sensation in the hand, reduced grip strength in the hand. Swelling or stiffness in the joints, Pain in wrists, forearms, elbows, neck, or back. Reduced range of motion in the shoulder, neck, or back. Dry, itchy, sore eyes or blurred vision.

Work-related MSDs can be prevented. Ergonomics -- fitting a job to a person -- helps lessen muscle fatigue, increases productivity and reduces the number and severity of work-related MSDs.

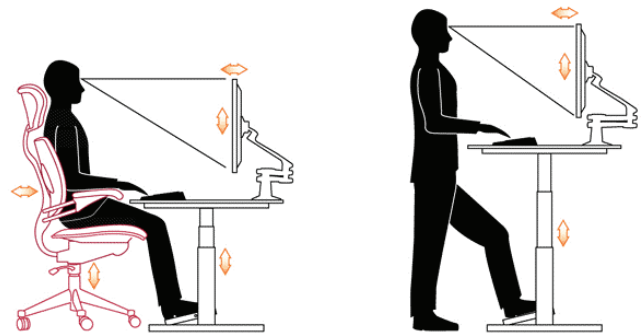
The following are important considerations when attempting to maintain neutral body postures while working at the computer workstation:

- Head is level, forward facing, and balanced. Generally it is in-line with the torso.
- Shoulders are relaxed and upper arms hang normally at the side of the body.
- Elbows stay in close to the body and are bent between 90 and 120 degrees.
- Hands, wrists, and forearms are straight, in-line and roughly parallel to the floor.
- Back is fully supported with proper lumbar support when sitting vertical or leaning back slightly.
- Thighs and hips are supported and generally parallel to the floor.
- Knees are about the same height as the hips with the feet slightly forward.
- Feet are fully supported by the floor or a footrest may be used if the desk height is not adjustable.

Regardless of how good your working posture is, working in the same posture or sitting still for prolonged periods is not healthy. You should change your working position frequently throughout the day in the following ways:

- Make small adjustments to your chair or backrest.
- Stretch your fingers, hands, arms, and torso.
- Stand up and walk around for a few minutes periodically.
- Perform some of your tasks in standing: computing, reading, phone, meetings.

These reference postures are examples of body posture changes that all provide neutral positioning for the body.



Upright Sitting Posture

Standing Posture

Upright sitting posture. The user's torso and neck are approximately vertical and in-line, the thighs are approximately horizontal, and the lower legs are vertical.

Standing posture. The user's legs, torso, neck, and head are approximately in-line and vertical with feet slightly apart. The user may also elevate one foot on a rest while in this posture.

MSD prevention. Your risk of developing MSDs increases with age. Your muscles, bones, and joints naturally deteriorate as you get older. But that doesn't mean that MSDs are inevitable. By taking care of your body throughout adulthood, you can lower your risk of developing these disorders. That's why it is important to develop healthy lifestyle habits now. Regular strengthening exercises and stretching can help keep your bones, joints, and muscles strong. It's also important to complete everyday activities in safe ways. Maintain a tall posture to prevent back pain, be careful when picking up heavy objects, and try to keep repetitive motions to a minimum.

References and Sources:

Occupational Safety and Health Administration
WebMD



Why I Stay...In the Fight!



Staff Sgt. Noah Gray, Echo Company, 782nd Military Intelligence (MI) Battalion, reenlisted in the U.S. Army for an additional six years because he wanted to 'give back' to the Soldiers and Army in appreciation for the opportunities he was given. Capt. Joseph Stanley, commander, Headquarters & Headquarters Company, 780th Military Intelligence Brigade, administered the Oath of Reenlistment and presided over the ceremony. (Courtesy photos)

FORT GEORGE G. MEADE, Md. -- Staff Sgt. Noah Gray, a cyber operations specialist assigned to Echo Company, 782nd Military Intelligence Battalion (Cyber), reenlisted in the U.S. Army for an additional six years.

His spouse is Mary Elizabeth Gray and she is a choral director at Meade Middle School.

Staff Sgt. Gray's hometown is Weatherford, Texas, and he joined the Army on January 24, 2011.

When Staff Sgt. Gray was asked why he reenlisted he said:

"I actually worked for Booz Allen Hamilton for about a month while I was on ETS (expiration term of service) leave. During that time my father (Lonnie P. Gray) was a big reason I reenlisted. While not a military member himself he saw all the great benefits of the military and what it had provided Mary and I."

"My father was constantly trying to convince me to reenlist even after I had accepted the job with

Booz Allen Hamilton."

"After about three weeks of contracting I came home one night and Mary noticed that I seemed unhappy with my new employment. I told her I missed the camaraderie of the unit, I missed the challenge of working more than one problem, and most of all I missed being a servant to those around me and helping them succeed."

"The Army has given Mary and I so much. It has provided us with countless opportunities that we otherwise would not of had."

"Some of my goals during this enlistment are to start giving back and providing other Soldiers with the types of opportunities I was afforded."

"I would also like to start stepping into some organizational leadership roles within the company (E Co. 782nd)."

"As a recently promoted Staff Sgt. I have just taken up the mantle as an alternate retention NCO. I think my unique experience can bring a different perspective to Soldiers on the fence about re-enlisting."



**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 Standing
Commercial: 301-677-4088



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



VIPs visit the Brigade



780 MI BDE CDR greets the CYBERCOM Vice CDR

FORT GEORGE G. MEADE, Maryland – Col. John “Dave” Branch, commander of the 780th Military Intelligence (MI) Brigade, greets Lt. Gen. William Mayville, Jr., Vice Commander, U.S. Cyber Command, outside the brigade headquarters, September 19. Mayville was here to receive an update from ARCYBER and the 780th MI Brigade on Cyberspace Operations. (U.S. Army Photo)



Army Chief of Staff gets cyber update

FORT GEORGE G. MEADE, Maryland – Army Chief of Staff Gen. Mark A. Milley (center, pointing) discusses Army cyber and network operations with Maj. Gen. John W. Baker, commander of the Army Network Enterprise Technology Command (right, pointing) and senior cyber leaders, at 780th Military Intelligence Brigade headquarters at Fort Meade, Md., Oct. 18. (U.S. Army Photo by Charlie Stadlander)



The Maryland Chapter of Heroes on the Water

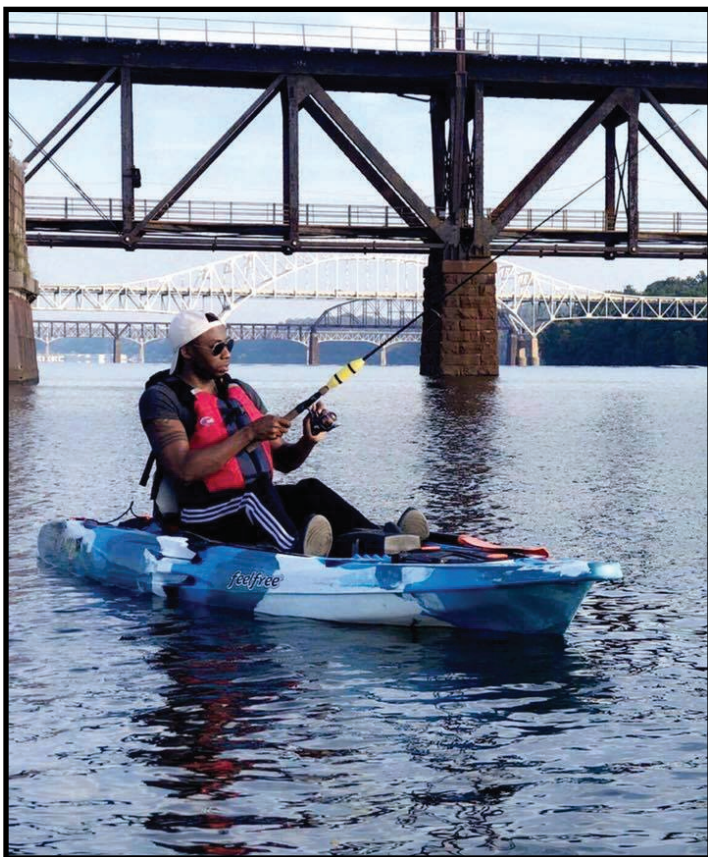
By James (Coop) Cooper, 780th Military Intelligence Brigade (Cyber)



FORT GEORGE G. MEADE, Md. – The Maryland Chapter of Heroes on the Water, or MD HOW is looking forward to 2018 and building upon its five-year history of providing kayak fishing events for the 780th Military Intelligence (MI)

Brigade and the Department of Defense.

So far, MD HOW has run events for the 782nd MI Battalion, headquartered at Fort Gordon, Georgia, the Headquarters and Headquarters Company (HHC), 780th MI Brigade, and E Company, 782nd MI Battalion, based at Fort Meade. Last year the Chapter even pulled their trailers, loaded with kayaks and fishing gear, and traveled to Fort Gordon to help jump start the Fort Gordon Chapter of Heroes on the Water. To make this happen, the MD HOW planned and conducted an event for the 782nd MI Battalion.



Over the past several years, MD HOW has taken E Company and HHC, 780th MI Brigade, as well as other Maryland-based military units to several fishing locations across the state. They targeted bass, stripers, perch, catfish and many other fish species, but their primary target was ensuring the service members had a great day on the water. MD HOW chapter volunteers are highly experienced and their objective is to take military and civilians who have never fished or been on a kayak before,



and ensure everyone has a safe and enjoyable experience. They have coordinated with the Brigades' Chaplains, and the chain of command to get the word out in order to put these events on. The events typically take place on a Friday requested by the specific unit, but the troops and civilians are always welcome at the monthly open events as well. There are no limits as to how many times they can participate. There are no memberships and no one will ever get a sales pitch. HOW is nonprofit and does not represent any product or manufacturer. What they do is support our military and first responders – anyone who has served is welcome.



Heroes on the Water is a nonprofit organization made up of over 86 chapters in over 36 states. Each Chapter is comprised of a 100 percent volunteer force and is made up of veterans and civilians from all walks of life who appreciate our military and want to say thank you.

The Maryland Chapter is starting its fifth year of operation in 2018 and looking forward to building upon its very successful outreach program. Jim Cooper and his leadership team started out with 10 kayaks and a few volunteers the first year and have grown to over 30 kayaks, 3 trailers and all the necessary fishing gear divided between the main chapter and their new subchapter, the Appalachian Chapter, which covers western Maryland and the West Virginia panhandle. The HOW volunteers



are made up of active duty, veterans, as well as civilians who have never served – in the Maryland Chapter you have surveyors, administrative clerks, contractors, grandmothers, and firemen. All walks of life are represented. They share a common appreciation for the military and what they do to protect our nation and constitution.



The organization has a twofold mission. Maryland HOW works with the Adaptive Rehabilitative Sports Specialists at Walter Reed National Military Medical Center, the Veterans Administration Hospitals and clinics, to provide these services to our nation's wounded service members and their families.

Just as important to helping our wounded service members is our dedication to thank our active duty, veterans, first responders and their combined families by taking them kayak fishing for free.





Army developing Expeditionary Cyber Teams to support

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



FORT IRWIN, Calif. – Soldiers from the Expeditionary Cyber Support Detachment (ECSD), 782nd Military Intelligence Battalion (Cyber), based out of Fort Gordon, Georgia, provide offensive cyber operations in support of the 1st Stryker Brigade Combat Team, 4th Infantry Division, during a seizure of a town at National Training Center Rotation 18-03, January 18. (U.S. Army photo by Capt. Adam Schinder)

FORT IRWIN, Calif. – U.S. Army Cyber Command is deploying Expeditionary Cyber-Electromagnetic Activities (CEMA) Teams (ECTs) in support of tactical commanders at the National Training Center (NTC) and their CEMA operations have become little different than real-world operations.

CEMA is an Army initiative designed to provide tactical commanders with integrated Department of Defense Information Network (DODIN) operations, Electronic Attack (EA), Electronic Protection (EP), Electronic Warfare Support (ES), Spectrum Management Operations (SMO), Intelligence, and Information Operations (IO) support/effects.

According to Maj. Wayne Sanders, the ARCYBER chief for CEMA, success for the Brigade Combat Team (BCT) in the cyber domain begins at the D-180 planning conference – 180 days before the unit's NTC rotation.

“The biggest thing for the D-180 are the key leader engagements,” said Sanders. “(At those conferences) we can inform the brigade commander about what types of CEMA support we can provide to help him shape conditions for his battle to be able to close with and destroy the enemy.”

Sanders said while he doesn't expect much from the BCT in terms of cyber activity, he does expect the commander and the staff to have an initial understanding of the CEMA environment and to provide their higher headquarters with a CERF (cyber effects request form). He mentioned that if the brigade plans for it correctly, for an expeditionary CEMA capability to be brought out to support

their operations, “then we can provide that for them.”

“If you're looking at this from a real-world perspective, if they identify that they are going somewhere in the world – somewhere they would need additional capacity that they may not have coverage for – they can submit that through a CERF, as a request for forces,” said Sanders. “And the beauty of the Expeditionary CEMA Teams is their scalability and reach back.”

Sanders explained the ECT concept originated from the Chief of Staff of the Army who directed the Cyber Support to Corps and Below Pilot in 2015. The pilot tasked ARCYBER to assess the best package of equipment, capability, authorities and personnel to support a BCT.

“That's why, out of the DOTMLPF-P (Doctrine, Organization, Training, Materiel, Leadership and Education, Personnel, Facilities and Policy) came the need for a force that provides the authorities, the senior and master level expeditionary cyber operators, and a quick turn cyber development capability, that doesn't exist right now in the Army,” said Sanders. “It provides infrastructure support personnel that

tactical commanders

can provide the same thing as having people on the ground.”

Sanders explained the goal is an Initial Operational Capability (IOC) requirement from the Chief of Staff of the Army, Gen. Mark Milley, in Fiscal year 2019.

Sgt. Maj. Jesse Potter, the operations sergeant major for the 780th Military Intelligence Brigade (Cyber), mentioned that although this is the ninth rotation since 2015, it has only been in the last three, including the ECT support to NTC Rotation 18-03 and the 1st Stryker Brigade Combat Team, 4th Infantry Division (1-4 SBCT), which occurred from January 18 through 24, that the ECT operations have begun to take shape and closely mirror real-world operations.

“We’ve learned that we were a very large logistical burden to the rotational training units. We learned our lessons about the CEMA capability that we can provide to a rotational training unit, and at the same time we were reducing the logistical requirement to provide that capability,” said Potter.

That reduces their footprint, giving commanders ways to choose between a “flyaway kit” with light capability, or more sustained cyber-electromagnetic operational need, Potter said.

Potter also mentioned another area ARCYBER was looking at was CEMA support at the division and corps levels.

“What’s missing, what’s next, is the division and corps level exercises. Enabling the education of the commanders through the institutional arm of the Army, which is primarily the mission of the Cyber Center of Excellence (CCoE). That is what the CCoE is working toward –incorporating CEMA into all aspects of the PME (Professional Military Education),” said Potter. “And then for the higher level exercises, just like we’ve done for the NTC rotations, how does the staff enable cyber based effects that supports the commander’s objectives, and what can they gain from having the cyberspace capability that they currently don’t have. Because at the same time, that education will benefit the brigade combat teams.”

Furthermore, ARCYBER is not just looking at the

development of the ECT structure and incorporating that support at the division and corps levels, the command is also determining the organizational structure to command and control those ECTs.

“Regarding the ECT structure...you have individuals, put together as a team, predominantly from four separate organizations across three MACOMs (Major Commands) – ARCYBER, Intelligence & Security Command, and the Cyber Center of Excellence,” said Potter. “Moving to an organizational structure whereby the ECTs are part of a larger unit as the force structure solution means we no longer have an organization that’s made up of a hodge-podge of people, further exasperating the issues that we have with the rotational training unit.

Potter and Sanders said that’s where they are now. Organic ECTs, all assigned to the same unit, and subordinate to ARCYBER will provide the Army with an expeditionary CEMA capability.

In summation, ARCYBER used the lessons learned from the past nine NTC rotations to determine the optimized force structure they are proposing to the Army to stand up an organization with all those separate elements that were under different commands, to fall under one command with CEMA capabilities tailorable to meet the tactical commander’s objectives.



FORT IRWIN, Calif. – Spc. Victorious Fuqua (on the computer), and Staff Sgt. Isaias Laureano, both cyber operations specialists from the ECSD, 782nd MI Battalion, provide offensive cyber operations, while Spc. Mark Osterholt pulls security, during the NTC Rotation 18-03, January 18. (U.S. Army photo)



Cyber activities at the National Training Center

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



FORT IRWIN, Calif. – Maj. Wayne Sanders, chief, Cyber Electromagnetic Activities (CEMA) Support to Corps and Below (CSCB), U.S. Army Cyber Command (left), and Sgt. Major Jesse Potter, the S3 operations sergeant major for the 780th Military Intelligence Brigade (Cyber) (right), watch as Spc. Justin Longshore, a cyber operations specialist assigned to the 782nd Military Intelligence Battalion (Cyber), controls a quad copter as it maneuvers towards a U.S. Army unit before it is ‘attacked’ by an anti-UAS (unmanned aircraft system) capability as part of the CSCB program during the 1st Stryker Brigade Combat Team, 4th Infantry Division, National Training Center Rotation 18-03, January 18 through 24. (U.S. Army photo)

FORT IRWIN, Calif. – U.S. Army Cyber Command (ARCYBER) is using the Cyber Electromagnetic Activities (CEMA) Support to Corps and Below (CSCB) program at the Combat Training Centers to develop and test CEMA concepts and operational cyber support to echelons corps and below.

The lessons learned from the CSCB support to the National Training Center’s rotational training units (RTUs), Opposing Forces (OPFOR) and Operations Group, have resulted in numerous milestones to include defensive cyber counter fire and systems that disrupt and neutralize unmanned aircraft systems (anti-UAS).

According to Sgt. Major Jesse Potter, the S3 operations sergeant major for the 780th Military Intelligence Brigade (Cyber), it has really only been in the last three rotations, including the CSCB support to the 1st Stryker Brigade Combat Team (SBCT), 4th Infantry Division, National Training Center Rotation 18-03, January 18 through 24, that the program has advanced to the point whereby the tactical training mirrors real world operations.

“Having been involved in all the previous CSCB rotations – and every rotation is a learning event – one of the big learning points is, in this specific rotation, the use of cyber enabled kinetic effects,” said Potter. “That is, the commander understands cyber is not only good for intelligence, but provides him with a sensor to shooter link that he is able to then leverage against High-Payoff Targets (HPTs). In other words, using cyber to gain access, to be able to see HPTs, and then to use that in concert with other capabilities to be able to geographically locate and neutralize HPTs is a technique that had not been done in previous rotations”

Maj. Wayne Sanders, the ARCYBER chief for CSCB, explained how. He said the Defensive Cyber Operations (DCO) team was noticing anomalous activity on the brigade’s network at certain times – usually late at night. The brigade also knew who the cyber threat actors were, and the brigade intelligence section (S2) knew one of these threat actors was seen in the vicinity of the Wi-Fi cafes during those hours, but because the S2 wasn’t reporting that through the operations channels and the communications (S6) wasn’t either, they never put the two together.

“That is where that CEMA piece is so critical, because otherwise intelligence stays in the S2 channels, and communications stays in the S6,” said Sanders. “This is the CEMA’s job and the Expeditionary CEMA Teams (ECTs) provide that extra expertise that leverages the higher level capabilities, such as the RCCs (Regional Cyber Centers), and the JCC (Joint Cyber Centers), and through the IC (Intelligence Community) – the result is more arrows in the commander’s quiver to generate effects.”

supports real world operations

Potter stated that in all the previous rotations the DCO perspective was focused on DCO IDM (Internal Defensive Measures), which includes hardening the network and monitoring activity in the network, part of information assurance.

“No rotation has done, up until this rotation, any type of semblance of a DCO counterfire,” said Potter. “To identify the target, being able to characterize the target, and then being able to make the transition from making an internal threat assessment, to making a request to target that individual as a process.”

Potter and Sanders both remarked on another significant achievement during this rotation which was the anti-UAS capability.

“There were UAS threats in the area that the OPFOR possessed that we did not have a capability for. We then turned around, tasked our ARCYBER enterprise to create a capability against those other threats, and that’s the model that we want to use,” said Sanders. “We don’t have to get into version numbers, because that gets into specifics, but it’s important to note that the Army has figured out, no matter where they go, we want to use the intelligence community to tell us what types of threat are out there so we can use our enterprise to create capabilities against that.”

According to Sanders, the COG, the Commander of Operations Group, is able to change the training scenario with as much, or as little cyber play as the COG wants, usually depending on how the brigade is doing in the fight, and, the OPFOR having a UAS capability is a real world scenario.

“The primary purpose for what we’re doing is to build confidence in the anti-UAS equipment. That it can actually function as the unit is told it can function, so when the Army deploys into theater they will actually have the real world capability to know – they have seen it work in testing – so they know that it works and they’ll actually deploy it,” said Potter.

Potter went on to say that is why a capability developer is critical to the ECT force structure.

“From the ECT perspective, this helps prove the concept of why the capability developer is so critical to

the ECT,” said Potter. “Because when they arrived they had a mission to defeat quad copters, but when they realized the capability they had didn’t work against the copters being employed the team turned to the Soldier on site with the ability to do on-site developing to determine what needed to be done to modify it so that they were able to defeat the enemy’s modifications.”

Sanders summed it up this way, “Our goal is to make sure that it actually works, the secondary piece is that in the future rotations we don’t want this to be our job as pilots either. The RTU gets the capability for a counter UAS capability, and we allow the OPFOR to fly their quad copters and either it gets worse for the RTU, or it doesn’t depending on how the brigade does.”



FORT IRWIN, Calif. – Staff Sgt. Jason Lott controls an quad copter as Warrant Officer Felipe Tristan observes during NTC Rotation 18-03. (U.S. Army photo)



ECSD provides offensive cyber operations

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



FORT IRWIN, Calif. – Soldiers from the Expeditionary Cyber Support Detachment, 782nd Military Intelligence Battalion (Cyber), provide an offensive cyber operations capability as part of the Cyber-Electromagnetic Activities (CEMA) Support to Corps and Below (CSCB) program during the 1st Stryker Brigade Combat Team, 4th Infantry Division, National Training Center Rotation 18-03, January 18 through 24. (U.S. Army photo)

FORT IRWIN, Calif. – Soldiers from the Expeditionary Cyber Support Detachment (ECSD), 782nd Military Intelligence (MI) Battalion (Cyber), based out of Fort Gordon, Georgia, are providing Cyber-Electromagnetic Activities (CEMA) support to a Stryker Brigade Combat Team from Fort Carson, Colorado, during National Training Center Rotation 18-03, January 18 through 24.

According to Staff Sgt. Isaias Laureano, a cyber operations noncommissioned officer assigned to the ECSD, the detachment conducted close access offensive cyber operations (OCO) in support of the rotational training unit.

“The 1st Stryker Brigade Combat Team, 4th Infantry Division, is conducting operations against a near-peer adversary threat and we are supporting them with our offensive cyber effects as part of the CEMA Support to Corps and Below (CSCB) program,” said Capt. Adam Schinder, a team leader with the 782nd MI Battalion ECSD. “(With) the offensive cyber operator team that we brought out here, we’re able establish connection and provide access for future operations and provide exploitation tools that we brought with us – so denying

the adversary the use of the internet, locally, and in the area of hostilities.”

Schinder said his team is also able to support the brigade in the deep fight.

“The brigade commander’s fight is the deep fight. If he can diminish the enemy’s combat power as they maneuver in zone than what he is doing is setting his battalions up for success,” said Schinder. “We’ve enabled that extremely well during this rotation – really showing the maturity of CSCB as a program.”

Schinder was referring to the team’s cyber operations specialists being able to observe a High-Payoff Target on the brigade commander’s High-Payoff Target List, deep in the opposing forces rear area, and enabling the unit to call in a deep strike to destroy it.

Schinder said there are some constraints with regards to the Law of Armed Conflict; however, everything his team accomplished was reviewed in accordance with the ROE (rules of engagement). He summed it up by remarking that “the ability for a brigade commander to have a national asset, task organized to him, and at his fingertips to employ them in the field to create effects is vital.”



Lightning Forge 18-01

By Capt. Adam P. Schinder, commander, Expeditionary Cyber Support Detachment, 782nd Military Intelligence Battalion

Lightning Forge 18-01: Insights and Lessons Learned from Integrating Cyber into Light Infantry Training



**SCHOFIELD
BARRACKS, Hawaii**
– Col. Dave Branch,
commander of the 780th
Military Intelligence (MI)
Brigade, authorized the
formal task organization

of the Expeditionary Cyber Support Detachment (ECSD) under the 782nd MI Battalion on March 31, 2017 with its primary mission to inform the CEMA (cyber-electromagnetic activities) Support to Corps and Below (CSCB) program on the requirements for conducting offensive cyber operations (OCO) on the operational and tactical edge.

Since its organization, the ECSD has participated in three home station trainings (HST), one partnered National Training Center (NTC) rotation with 781st MI Battalion, and two other NTC rotations as the sole executor. This article discusses the insights and lessons learned from the HST event Lightning Forge 18-01 (LF 18-01) with 3rd Infantry Brigade Combat Team, 25th Infantry Division (3/25 IBCT), based out of Schofield Barracks, Hawaii.

Lightning Forge is the annual culminating training event for units assigned to the 25th Infantry Division (ID). It is held in training areas around Hawaii, with LF 18-01 localized to the training areas around Schofield Barracks on Oahu. The training highlights dismounted maneuver through a harsh tropical environment. Unlike the rotations the ECSD had supported at the NTC, the training area in Hawaii has steeper valleys, no in-place network architecture, and it is riddled with thick canopy that degrades line of sight communications. Light units are always the most challenging for the ECSD to integrate with, but the environment compounded these challenges. To meet these challenges, the ECSD leadership modified their training, equipping, and the exercise regimen to accommodate the introduction of Cyber effects.

The ECSD leadership met with the Army Cyber Command (ARCYBER) Chief of CSCB, Maj. Wayne Sanders, on an initial leader's reconnaissance of the training area the final week of August. There the team clarified the division commander's intent for training and established a timeline for execution.

The 25th ID commander always seeks to build complexity on each iteration of Lightning Forge, with a key emphasis placed upon enabling the training unit with new assets and capabilities. In doing this, the staff of 25th ID solicited input from ARCYBER and the ECSD to modify LF 18-01 in order to integrate Cyber effects. The result was that the ECSD would emulate a peer adversary mission command node for targeting and possible exploitation. This was a new concept in that the training exercise enabled the CSCB program to demonstrate the value of expeditionary cyber in compromising enemy operational facilities. In addition, the ECSD discussed establishing proximal access in the field to enable remote operations and planned for the execution of remote web operations on their representative internet from a simulated CMT (Cyber Mission Team) or JMOC (Joint Mission Operations Center). Remote operations would need to be simulated in the case of LF 18-01 for lack of a closed network. After this site visit, the ECSD had only six weeks to prepare for the training event.

(Continued on the next page)



LIGHTNING FORGE 18-01. Hawaii -- ECSD operators show electronic warfare noncommissioned officers with 3/25 IBCT the stripped down equipment – the equipment was covered for weatherproofing.



Lightning Forge 18-01 (continued)

(Continued from the previous page)

Our kit had to be light, the operator's needed to be fit, and a target network needed to be designed.

Providing support at the NTC is challenging; however it is convenient to be able to pack a bunch of items into pelican cases and throw them in a Humvee for the operator team. In this case, our expeditionary cyber operators would be rucking up mountainous terrain to gain observation of the enemy with the Scouts of 3/25 IBCT. Knowing this, the ECSD leadership directed the team to strip down the kit for our OCO operator teams to the bare essentials to establish a light infantry version. In addition, the NCO in charge of the OCO operator team implemented a physical training plan that involved two ruck marches a week with increasing difficulty and the operators triaged what was essential for close and proximal access operations.

The development team NCOIC, under the direction of the ECSD chief technical officer, was tasked with designing and fielding the target network that the operators would attempt to identify and exploit in the field. Within three weeks the ECSD's internal development team designed, tested, and deployed a "fly-away" network that models a small enterprise complete with networked services and a firewall between the simulated unclassified and simulated classified network. Maj. Marlon Mallory, commander of Detachment Hawaii (Det.-HI), 782nd MI Battalion, advised the ECSD development team to create a design loosely based on a WIN-T model for speed of development. The team decided to design a network with Windows hosts managed by a domain controller – complete with migrating profiles and active directory share services. ECSD development technicians installed, configured, and debugged this network, demonstrating the capability of a rapid fielding effort.

When in the field, having a physical network, rather than a virtual environment is crucial. Virtual training cannot engage OCO operators in the field to perform terrain analysis, conduct a wireless survey, positively identify a threat network, locate it, navigate

to it, and compromise it – it has to be a physical network. This allowed the OCO operator team to train identification of a network of interest and to be prepared to conduct rudimentary digital forensics should the devices be captured by friendly forces.

During LF 18-01 the ECSD supplied this network to the OPFOR (opposing forces) unit -- 1st Battalion, 27th Infantry Regiment (1-27 IN)). At the request of ARCYBER, the 25th ID advised 1-27 IN to employ the network as a company command post or Battalion TOC (tactical operations center) on the battlefield. More importantly, they required the unit to use it for operational planning or to load it with documents pertaining to their various staff functions. The development team assumed the role of infrastructure support, as is usually the case in training. Consistent with the requests of the OPFOR commander, they established the network wherever the 1-27 IN TOC was located and kept it operational as a target for the ECSD operator teams.



LIGHTNING FORGE 18-01. Hawaii -- *The Development Team's simulated adversary network.*

Det.-HI augmented the ECSD operator teams with three Soldiers, and along with the plans team they made link-up with 3/25 IBCT for Receiving Staging and Onward Integration (RSOI). Integrating with the staff of 3/25 IBCT was less difficult as compared to previous staff encounters. The brigade commander, Col. Robert Ryan, was excited to receive the team and to leverage every capability we had against the enemy. As a former commander within JSOC (Joint Special Operations Command), he understood the value of technical advantage and instructed us to work with his staff to target every weakness of the enemy.



The brigade CEMA officer shared this vision and quickly engaged the ECSD plans team in Mission Analysis with the staff. The staff had just returned from Cyber Blitz with a fresh understanding of mission command shortcomings and displayed a keen desire to develop the enemy picture with the operator teams as a reconnaissance asset. After drawing their equipment the ECSD team deployed with the Brigade TOC to Dillingham Airfield on Oahu and task organized the OCO operator teams to the 3/25 IBCT Scout Squadron to begin rehearsals for actions on the objective.

The physical conditioning and technical training paid off. The 3/25 scouts never had to stop for our team while maneuvering in the mountainous terrain. In addition, the team was able to locate the enemy mission command node and notify the scouts before friendly forces compromised their position by maneuvering too close. Using open-source tools, the team was able to recover a wireless handshake and run through a handful of dictionaries to quickly break the encryption and associate with the wireless network. After establishing access, the team classified the attached devices and scanned the machines for vulnerabilities. After identifying a few potential candidates for vulnerable services, the operators attempted exploitation until they achieved success.

In this case, the team was able to access the network and one device attached to it within less than two hours. This was mostly due to the luck of having a few dictionaries on hand to associate with the wireless AP, including some specially made in the field using a tool called “crunch” for generating brute-force lists when the password policy is understood. After initial exploitation, the team recovered as many files as possible before the scouts indicated it was time to go. Before leaving, the team configured the WAN (wide area network) firewall to deny all traffic and disconnected.

The team now needed to get the intelligence back to

the OCO plans team at the Brigade TOC. This required a ground convoy to be assembled, with the whole process taking approximately 24 hours. Had the team been fielded robust out-of-band data communications, transferring data back to the Brigade TOC could have been occurred more rapidly.

Regardless, after returning the OCO operator team burned a handful of CDs and distributed them to the brigade S3 (operations), brigade S2 (intelligence), and CEMA staff. On it they had the enemy’s most recent commander’s update brief, battle update brief, scheme of maneuver, communications cards, and location of C2 and logistics nodes. It was a hit! The staff immediately began targeting, with the first mission ordered being the capture of the enemy retransmission station. Given the complete picture of the enemy, the operation went very well and the brigade continued the fight with a renewed lethality that only a clear picture of the enemy can provide. The value of validating the S2’s assumptions in real time was clear to the staff.

Given the issues with attempting connection from the ground with the brigade scout squadron, the brigade CEMA Officer and OCO plans team drafted a CONOP (concept of operations) to attempt a second proximal access operation, this time from the sky.

(Continued on the next page)



LIGHTNING FORGE 18-01, Hawaii - The ECSD training for airborne operation.



Lightning Forge 18-01 (continued)

(Continued from the previous page)

The OPFOR was equipped with a healthy amount of anti-aircraft detection and attack capabilities, with the principle threat being three air defense missile systems. Knowing this, the CONOP called for the OCO operator team to fly in a U.S. Blackhawk helicopter outside the range of the ADA (air defense artillery) system, and connect using our equipment. It was approved by the brigade commander, and the team immediately began cold-load training.

The team configured their equipment for flight, tied everything down, and waited for clearance to fly. Unfortunately, the mission never took place due to paperwork issues. Despite this, the team

has at least cold-load trained the TTPs (tactics, techniques and procedures) required for this mission and we look forward to executing it in future operations.

Lightning Forge was a unique and valuable opportunity to be a part of both the exercise control staffing and the training audience of a major exercise. It challenged our operators to lighten their rucks, get fit, and quickly conduct actions on the objective; it challenged our developers to deploy an attack surface for a threat mission command node; it challenged our plans team to think of new and innovative ways to design training and employ the ECSD operationally; it challenged the Soldiers we received from Det.-HI to work with our team outside their normal roles; and most importantly, it highlighted gaps in our equipment and tactics.

Overall, the experience was priceless and the team grew. In the future, we will continue to improve the simulated mission command node to more closely replicate real peer adversary C2 nodes, complete with a translation of all documents to another language. We also identified our most important material fielding concern – the need for better



The ECSD and partners. left to right: 1st Lt. Aaditya (Sunny) Bhatia, Spc. Mark Osterholt, Spc. Victorious Fuqua, Staff Sgt. Isaias Laureano, Spc. Lopez, Sgt. 1st Class Alexander Simon, Staff Sgt. German, Staff Sgt. Mubarak, Sgt. Currey, Capt. Adam Schinder

communications equipment. In particular, man-portable and vehicle mounted systems that can send data out-of-band from our operators in the field to the plans team in the TOC.

For the past ten months I have had the distinct honor and privilege of being the first to command the OCO arm of the CSCB pilot as the detachment commander of the Expeditionary Cyber Support Detachment. As part of a continuing program to optimize the delivery of skilled cyber operators and advanced capabilities to the tactical edge of combat, the CEMA Support to Corps and Below program is maturing quickly. The program's initial problem statement was roughly, "How do we combine the talents of skilled Soldiers from offensive cyber operations, defensive cyber operations, electronic warfare, psychological operations, and information operations and deliver these talents to the operational and tactical edge where they are needed?" Each of these domains exist under separate guidons, and recent investigation suggests that a blended organization provides more value to a supported ground combat Commander.

ARCYBER has proposed a plan for a blended organization as early as fall of this year.

IN REMEMBRANCE OF SGT. 1ST CLASS TOMMY L. ROBINSON



Sgt. 1st Class (SFC) Tommy L. Robinson, Jr., was born in Florida to Narzell Robinson and the late Tommie L. Robinson. He spent most of his formative years in the small town of Campbellton, Florida, where he graduated from Graceville High School Class of 1985 and was well known for his stardom in Track and Field. He later moved to California and attended San Diego City College and attained an Associate's Degree. There he fell in love with and married Irma Glenda and together they have two beautiful children, Khaleed, and Kiera.

SFC Robinson was an honored and celebrated Soldier with over 24 years of Active Duty Service in the United States Army. Under the guidance and mentorship of his brother, David Robinson, Tommy achieved much during his stellar Military career. Becoming a Drill Sergeant and completing Protocol Officer Certification in 2016 are among Tommy's most cherished accomplishments. He was charged to mold and guide young civilians into disciplined Soldiers. Tommy had the opportunity to serve at various locations throughout his military career including: Afghanistan (Operation Enduring Freedom); the White House Communications Agency, D.C.; Fort Meade, Maryland; Fort Sill, Oklahoma; the Joint Staff Pentagon, Fort Hood, Texas; Fort Sam Houston, Texas; and ultimately the Warrior Transition Brigade, Walter Reed National Military Medical Center.



SFC Robinson was a valued member of the 780th Military Intelligence Brigade from August 9, 2013 to July 19, 2017. He worked in many sections throughout the Brigade including: a Cyber Protection Team, the noncommissioned officer-in-charge of the S6 section, and in S3 CUOPS (current operations). He was affectionately known as "The Voice" across the Brigade for his amazing voice; he was always requested to support different ceremonies throughout the organization.

SFC Robinson was surrounded by Family when he passed away in the early morning of November 27, 2017.

Soldiers and Civilians of the Brigade were honored to attend and support his services at the Church at Severn Run, December 8, 2017. SFC Robinson is interred at the Crownsville Veteran's Cemetery, Crownsville, Maryland.





FORT GEORGE G. MEADE, Md. - Spc. Alan Kim, 780th Military Intelligence (MI) Brigade (Cyber), competes in the modified Army Combat Readiness Test portion of the Army Cyber Skill Challenge V, Nov. 16, 2017. The 780th hosted the competition, which included a physical and technical portion to encapsulate the total soldier concept. (U.S. Army photo By Spc. Elizabeth Brown)