Volume 6, Issue 2

# the BYTE

## 780th Military Intelligence Brigade

* Best Warrior Competition
* Task Force Echo Transition
* CyberPatriot X
* 781st MI BN CoR
* Accomplishments 2014-2016


"...In the Fight!"

The BYTE is a publication of the 780th Military Intelligence Brigade (MI BDE), 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 BDE 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...**



**On the cover:**
***FORT GEORGE G. MEADE, Md.***
*– Command Sgt. Maj. James Krog, the senior enlisted Soldier for the 780th Military Intelligence Brigade (Cyber), assumed responsibility as the "keeper of the colors" during a Change of Responsibility ceremony on a field near the brigade headquarters, September 8. (US Army Photo)*

# Features



# Articles



# Photo Pages



# From the Editor

The theme for this issue is *"...In the Fight"*

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

The 780th MI BDE, and its subordinate units, receive orders and tasking from multiple commands to include: U.S. Cyber Command (USCYBERCOM); the Cyber National Mission Force (CNMF); Joint Force Headquarters - Cyber (JFHQ-C) for Army, Navy and Air Force; U.S. Intelligence & Security Command (INSCOM); U.S. Army Cyber Command (ARCYBER); Fort Meade Garrison, and Fort Gordon Garrison.

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 Team. 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**

***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.

# "Everywhere and Always..."

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

This, my final entry in **the BYTE** as your Commander, is dedicated to each of those within the ranks of the 780th. For the last two years, I have watched as you collectively accepted the tough challenges of establishing our multiple teams and total force. To say that I am proud of you all is an understatement!

On the day I took command of the 780th, I exclaimed, "Wow!" in response to all the potential and energy I saw within this unit. As I depart command, I again exclaim, "Wow!" in response to all the efforts that I have witnessed. What once many considered impossible, now is considered difficult; what was considered difficult at one time is now routine; and the routine has simply become "easy." You have collectively shown a commitment that speaks to the intelligence, discipline, and determination required to achieve the impossible, overcome the difficult, and capture the routine. Doing so has made the 780th and each of you the consistent choice of senior leaders when the critical task cannot fail.

Reflection provides perspective and I wish to offer that here for a momentary relief from the continuously evolving work that lays ahead. So in reflecting, consider all that the 780th family achieved:

- Completed FOC of all teams and transitioned to Sustainable Readiness – leading U.S. Cyber Command (USCYBERCOM);
- Established and expanded two Joint Mission Operation Centers – leading USCYBERCOM;
- Integrated the largest Army National Guard mobilization(TF Echo) ever for USCYBERCOM;
- Established Cyber Solutions Development (CSD) Detachment and consolidated developers;
- Trained over 100 Developers and initiated a JQR process to test and advance capabilities;
- Grew the pool of Operators by partnering and instructing an Army Operator Course at the Cyber Center of Excellence (CCOE);
- Executed operations with tactical, operational, and strategic impacts;
- Informed the FY19 Cyber Warfare Support Battalion build through CSCB (Cyber Electromagnetic Activities (CEMA) Support to Corps and Below) efforts;
- Built and delivered capability to the current battlefields;
- Improved team and staff procedures resulting in consistently higher performance;
- Through AIP/SDAP, recognized and rewarded our advancing/improving population;
- Contributed greatly to our Sister Services and Higher Headquarters as part of the Enterprise

AND….

- Last and as important as any other measure – we did all this and more with dignity and respect!

These achievements are the work of a professional force. Each of you should be proud of your contributions.

I am proud to have served as your commander and will fondly remember the honor of being in your presence.

In a previous Byte I challenged each of you to "seek opportunities to contribute, seek daily to learn more about the cyberspace domain, and seek to improve the 780th MI BDE and our larger Joint Cyberspace Force." I challenge you now to continue that charge under your new leadership. And in your future endeavors, wherever they may take you, I hope you also willingly "contribute, seek and learn" as that will allow you to continue to be ***"EVERYWHERE AND ALWAYS…IN THE FIGHT!"***


# "...In the Fight!"

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

"In the Fight" – the perfect motto for this Brigade. The Soldiers of this Brigade are creative and innovative, always looking for better ways to do their jobs and help the team accomplish the mission regardless of whether it is supporting forces on the ground, responding to malicious activity on our networks, or conducting operations in support of national level authorities.

In the short amount of time I have been the Brigade CSM, we have:

- More than doubled our capacity and capability to support the fight;
- Expanded our Joint Mission Operations Center to enable an increased operations tempo;
- Continued to send our CEMA Support to Corps and Below team out to the National Training Center at Fort Irwin, California to support and train our Army's Brigade Combat Teams in preparation for their deployments;
- Established a state-of-the-art facility to support its capability development requirements and provide a home to the 781st Military Intelligence Battalion headquarters; and
- Deployed Soldiers and Civilians around the world to work with partners, increase our capabilities, and support the forces on the ground.

All of this is in addition to our assigned missions of supporting the Cyber National Mission Force, Joint Force Headquarters - Cyber, and the Combatant Commands.

We also on-boarded our second iteration of Task Force – Echo, the Army National Guard team that enables us to conduct our operational mission on a daily basis. While we are sad to see the current team go, it is exciting bring on their replacements and help them prepare for their state missions while they support our mission.

On the operational side, it is easy to see how this Brigade is "In the Fight" and will be for the foreseeable future, but let's not forget the support required to enable the operational elements to be "In the Fight" --

- The S1 processes the administrative actions including awards, evaluations, leave forms, and other actions for over 1300 personnel;
- The S2 processes the clearances and access requirements for the Brigade;
- The S3 processes all operations orders; runs the current operations and future operations; supports the operational mission with intelligence operations support; manages the individual, collective, pipeline, cyber, NCOPDS (Professional Development System), and all other training for the Brigade;
- The S4 ensures the teams have the equipment and supplies they need;
- The S6 sets up, configures, and connects the communications and computer equipment needed by many of the Soldiers and Civilians to accomplish their mission; and
- The Special Staff ensures our spiritual, mental, and physical readiness by providing counseling and training in the areas of SHARP, Equal Opportunity, suicide prevention, retention, and a myriad of other areas.

Without the support of these Soldiers and Civilians, it would be impossible for the Brigade to accomplish its operational mission. They are "In the Fight", taking care of the daily work needed to support and enable the Cyber Mission Teams of the Brigade to conduct cyberspace operations in support of the Nation, the Army, and the Combatant Commands.

I continue to be amazed by everything you do, you are truly ***"EVERYWHERE AND ALWAYS…IN THE FIGHT!"***

# Cyber Truths: If Everywhere is Important, Is Nowhere Important?

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

*"You will not find it difficult to prove that battles, campaigns, and even wars have been won or lost primarily because of logistics."* – Gen. Dwight D. Eisenhower

The 2018 Command Vision for U.S. Cyber Command tells us that we must now "scale to the magnitude of the threat, removing constraints on our speed and agility, and maneuvering to counter adversaries and enhance our national security". The Department of Defense is "building the operational expertise and capacity to meet growing cyberspace threats and stop cyber aggression before it reaches our networks and systems." It also asserts that our first imperative is to "achieve and sustain overmatch of adversary capabilities" and "ensure the readiness of the force."

But can we truly "scale" a high-demand, low-density maneuver force without ruthless prioritization?

When asked about the growth of Army Cyber with the junior enlisted members of the Vanguard Battalion, I cited the "SOF Truths" – humans are more important than hardware, quality is better than quantity, Special Operations Forces cannot be mass produced, competent Special Operations Forces cannot be created after emergencies occur, and most Special Operations Forces require non-SOF assistance. These statements are just as true if "cyber" is substituted for "SOF", and likewise we must remind ourselves of these "Cyber Truths" as we continue to grow the force with the Cyber Solutions Development (CSD) detachment, Advanced Education Program for Cyber Engineers (AEPCE), Cyberspace Operations Integrated Planning Elements (CO-IPE), Cyber Warfare Support Battalion (CWSB), Multi-Domain Task Force (MDTF), or other Cyber Electromagnetic Activities (CEMA) Support to Corps & Below (CSCB) initiatives that will ensure breadth is prioritized over depth for the foreseeable future in the Army Cyber Mission Force.

Although we have proven time and time again that we can do anything once, the ultimate test of a concept's viability is whether it can be sustained in the long-term. With a low-density work force that does not scale any better than SOF, depth must be prioritized over breadth if we are to do anything well in a repeatable manner. Otherwise, we end up in a continual and sometimes ineffectual state of "doing more with less".

These realities shape the context for Commanders who are charged with providing trained and ready forces to our operational commanders – not just one time to reach Full Operational Capability (FOC), but at all times for a force that is "in the fight" 365/24/7. For the past two years, in accordance with the Chief of Staff of the Army's number one priority of Readiness, we have maintained a persistent stare on the Resource Readiness of the 781st Military Intelligence Battalion, attempting to meet the Operational Readiness requirements of the Cyber National Mission Force (CNMF) while supporting Army Cyber priorities. Daily, however, we are confronted with the inescapable reality that every mission, initiative, requirement, tasking, etc competes for the same resources (manning, training, equipping), thus ensuring a congested and contested environment amongst friendly forces, not just with enemy forces.

This zero sum game ensures that any growth in one area will lead to degradation in another, and the reason, simply put, revolves around a lack of depth in what I consider our logistics base.

We lack depth in manning, our force structure is too junior in many areas to ensure we have seasoned experts operating at the National level and too often we rely heavily on "best athletes" that will eventually transition to other assignments without a bench to mitigate the turnover. Furthermore, the Army as a whole lacks a robust inventory of cyber professionals to mitigate losses to other sectors.

*Continued on page 36*

# "...In the Fight!"

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

As we enter a period of significant leadership change (and change of command speeches), I have reflected on how much the Battalion has done over the last year. The Battalion is, in every sense of the phrase, "Everywhere and Always…In the Fight!"

As you would expect, our teams, operations center, and developers are fully engaged in accomplishing their assigned missions. They have performed admirably. At this point last year, I would have told you that two mission teams were decisively engaged, four jogging along, and two awaiting an opportunity. Now, I would tell you that seven mission teams are engaged and one in transition. Both the mission teams and support teams are in the fight.

That said, solely evaluating "In the Fight" in terms of our assigned missions misses all the other wonderful things that happen within our Battalion. The following is a small sampling of other events that have occurred in the last quarter:

Our company level leaders continue to take care of their Soldiers, Civilians, and Family members. We have several company commanders and first sergeants departing and I would like to thank them for their efforts. A special thank you to: Capt. Hess, Capt. Ellis, Capt. Riddick, Capt. Jaimie, 1st Sgt. Harshman, 1st Sgt. Webber, and 1st Sgt. Tucker. Similarly, I would like to welcome the following to the company command teams: Capt. Clayton, Capt. Thursby, Capt. Buckles, 1st Sgt. Bozman, 1st Sgt. Fowler, and 1st Sgt. Milam to the team.

The Battalion staff, like the company level leaders, continues to provide excellent support to our Soldiers, Civilians, and Family members. All sections recently completed a brigade inspection/assistance visit and are preparing for an Intelligence and Security Command visit in July. These inspections validate our processes, but more importantly serve as a reminder that our staff knows their jobs and can provide world class support to our people. A special thanks to our staff primaries that depart this summer, especially Capt. Langley, Maj. Seales, and Capt. Paggett.

Chaplain White continues to spend time with our Soldiers and bless us with his inspired invocations at ceremonies. The Chaplain and Spc. Gallegos also continue to manage our Strong Bonds program. If you have not attended one or have not been in a while, I encourage you to attend. Finally, the chaplain has scheduled Applied Suicide Intervention Skills Training and is hosting a volunteer recognition ceremony on 8 June.

The Expeditionary Cyber Support Detachment completed "home station" training with a brigade from Fort Bliss, Texas. They taught the brigade staff and some of the subordinate units about Cyber Operations at the tactical level. They were incredibly successful and will spend late-May and early-June at the National Training Center continuing to build on that success. Best of luck to them.

The Soldiers of Detachment-Hawaii coached, taught, and mentored students from the Leilehua High School JROTC Cyber Patriot team. The Soldiers efforts enabled the team to qualify for Cyber Patriot X Nationals, after finishing first in their region.

Alpha Company maintains a special school relationship with the Sue Reynolds Elementary School. In early March, the Archers conducted an event called "Leaders as Readers," where Alpha Company Soldiers took time to read books to students. In another project, the Archers taught coding classes. The feedback from the teachers and students was outstanding.

Alpha Company, Bravo Company, and the Expeditionary Cyber Support Detachment recently ran a collective cyber exercise that included participants from the Cyber Protection Brigade and members of the Augusta University ROTC department.

*Continued on page 35*

# Servant Leadership

*By Staff Sgt. Brandon Lecocq, 781st Military Intelligence Battalion (Cyber)*


For as long as I can remember, I have always had a passion for helping others. Simple things like stopping on the side of the road for a disabled vehicle or making time to lend an open ear are a given, but it wasn't until I joined the military that I realized where that passion was coming from. There is a certain feeling of gratification that comes from being able to assist someone in need, as if you prevented them from some heartache, minute as it may be. That same passion is what drove me to become a servant leader. As a leader, you must be able to follow before you can lead effectively. In my opinion, in order to do both, you must learn to become a discerning leader. John C. Maxwell put it best, "true leadership must be for the benefit of the followers, not to enrich the leader."

Thus far in my career, I have been fortunate enough to participate in and create several events that were conceived to give back to the community. For example, in San Angelo, Texas, during my time at Advanced Individual Training (AIT), I was part of a team that ran over 500 miles in 24 hours for the community based fundraising event of the American Cancer Society, Relay for Life. I still talk about that event to this day where I made lasting memories, true friends, and most importantly helped save lives.

Similarly, in 2010, I devoted my personal time to train for and run in the Boston Marathon in support of the Boston Police Foundation by raising funds and creating long lasting relationships between the military and law enforcement communities. Both of these events, while distinctive in nature, proved to have kindred impacts to their respective communities. My thought process behind these types of events has always been to challenge myself, both mentally and physically while helping others.

Most recently, while stationed in Korea, I decided to again challenge myself physically while raising awareness on two topics that I have personally witnessed the impact of; veteran's transition assistance and suicide prevention among veterans. I decided to ride my bicycle over 400 miles across the South Korean peninsula to shed light on these two controversial topics within the veteran community and raised funds for a charity that has a direct impact on veteran's lives.

My experience is and will be vastly different from anyone else's. If you're interested in volunteering, there are numerous ways to do so and they do not have to be physical to have an impact or make a point. We have several volunteer coordinators spread throughout the formation, so all you have to do is ask! Volunteering can be extremely humbling as small changes can have a big impacts and I can promise you that you will learn something about yourself, while helping to keep others ***"...In the Fight!"***

# Cyber Development and Mentorship Exercise training series

*By Capt. Neil Milchak, commander, Headquarters & Headquarters Company, 781st MI Battalion (Cyber)*

As the Army's only Cyber Brigade engaged in the full spectrum of cyberspace operations, the Soldiers and Civilians of the 780th Military Intelligence Brigade (MI BDE) can truly be described as *"Everywhere and Always…In the Fight."* As the cyberspace domain is increasingly woven into devices, systems, and organizations resident in the land, sea, air, and space warfighting domains, combatants in the cyberspace domain including the 780th MI BDE will be able to bring the fight to the enemy along an ever-expanding multi-domain front, and with a growing magnitude of potential effects. Members of our Brigade train and prepare every day to deliver these effects against our Nation's adversaries.

However, the growth of the cyberspace domain brings the members of the 780th MI BDE into the cyberspace fight in another way, and it is not just our BDE's "on-keyboard" personnel that are affected. The connectedness that has transformed military operations and systems has also brought more of our personal lives, devices, and data online – placing us all on the cyberspace battlefield, and given the right motive and opportunity, making us the targets of our adversaries.

American Soldiers deployed to the Baltic States in support of NATO, as well as the soldiers of our NATO allies, experienced hacking attempts against their smartphones and electronic surveillance-enabled intimidation tactics when deployed near the Russian border in 2017. Recent data exposures, such as the 2015 OPM and the 2017 Equifax breach, have resulted in sensitive details about many of us falling into unknown (and in the case of OPM) likely state-sponsored hands. Social media shares and collects information about us that we provide, and as highlighted by the recent Cambridge Analytica scandal, there are many ways for third parties to access and exploit that information.

Many members of the Brigade, through the nature of their MOS (military occupational specialties) and work roles, are already familiar with these sorts of threats and take appropriate precautions to protect their devices and data. However, not all of the Soldiers and Civilians within our organization have the prerequisite knowledge or training to understand this threat and protect themselves. And in the face of daily news about data breaches and new exploits in the wild without immediately observable effects on your life, it is easy for anyone (even cyber experts) to become complacent when using convenient Online services.

In order to address this evolving training gap, Headquarters and Headquarters Company (HHC), 781st MI Battalion (MI BN) has developed the 781st MI BN Staff Cyber Development and Mentorship Exercise (CDMX) training series that focuses on online privacy, security, and OPSEC. The first course in the series was created to provide members of the Battalion Staff with hands-on, practical tips to protect themselves online. The course also provides an introduction to the cyberspace domain in a way that is more directly relatable to non-cyber members of the BN staff rather than focus on topics like penetration testing, incident response, or offensive cyberspace operations. While some portions of the instruction are review only for many cyber-MOS personnel, the privacy and persona implications discussed during the course are in many cases not covered extensively during MOS or CMF (career management fields) pipeline training.

# "ALWAYS in the Fight"

*By Capt. Skyler Onken, commander, A Company, 781st Military Intelligence Battalion (Cyber)*

The Brigade's motto is often read: *"Everywhere and Always... In the Fight."* I think experience has shown us that it is better read as *"Everywhere... and Always in the Fight."* Our conventional kinetic peers operate off of readiness cycles that permit them to transition through operational deployment, refitting and training. This model is proven to be effective and our entire warfighting mindset has been influenced by these lessons learned. With cyber being as young and unique as it is, we have not been able to rectify the nature of the war with the resource and operational requirements it necessitates.

Alpha Company of the 781st Military Intelligence Battalion has been experiencing an unprecedented operational tempo. With a nearly constant and uninterrupted stream of contingency operations and "surges" since 2014, the Soldiers of our company are being asked to sustain a level of readiness that the Army model is not built to maintain. A vast majority of the formation is dealing with conflicting prioritization of training and operations, spending necessary leave days, and maintains their private lives and families with no re-deployment in sight.

True to their name, the performance of the Alpha Company Avengers has been heroic. Through sheer will of force, military discipline and Soldiery perseverance, they have remained a formidable force in spite of the circumstances. Paving the way in technical, operational and policy battles, the Soldiers have proven themselves up to the challenge; they are truly ***"Always in the Fight."*** The task to all of us (for every Soldier is a leader) is to tease out the lessons to be learned: challenge the assumptions, apply sound doctrine, and ensure mission success.

As with anything new, we formulate our perspectives and adopt assumptions based on our experiences and training. However, confirmation biases are inevitable and our chief pitfall is a fear of challenging norms and tradition. The Department of the Army has recently set a good example by forcing a re-look at which annual training is actually applicable to ensuring our ability to win wars. We must ask ourselves the same thing. We find ourselves in a zero-sum game having to choose between good activities and best activities. With our limited resources, like time, are we spending it in ways that best get after mission accomplishment and victory. There are many good activities which we could be partaking in, but what are the best activities.

Carl von Clausewitz outlined the Principles of War which, when followed, best lead to victory. One of them, the principle of Economy of Force, states that we should *"Employ all combat power available in the most effective way possible; allocate minimum essential combat power to secondary efforts."* Being ***"Always in the Fight"*** we can easily get caught decisively engaged in tactical engagements. We must be watchful, recognizing when perspectives and actions, though expedient, de-couple or distract from the long-term strategy of a sustainable cyber force.

# Staying ready to "Fight Tonight!"

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

What precisely does it mean for a National Cyber Protection Team (NCPT) to be ready to ***"Fight Tonight"***? At face value, the two teams at Ft. Meade could argue they are ready because they are already in the fight today. However, this argument ignores the intricacies of what it means to be ready while being operationally engaged. Being ready to ***"Fight Tonight"*** is more than being ready for the current fight, it means being ready for the next fight.

One of the most difficult challenges the NCPTs at Ft. Meade face is making time to conduct collective training focused on future operations while maintaining progress on their current missions. It is easy to get lost in the current mission set and train with laser focus to accomplish that one task. However, we lose touch with the skillsets we are not using on that mission when we do this. If we do not make the time to train on these other skills, we may find ourselves unready for the next fight that could kick off at any time.

In order to get after this training, we have begun to leverage the Cyber Protection Brigade's model for task organizing the team into independent mission elements. By focusing at this lower level, we can keep one element engaged in the current fight while the other one takes time to train against the next one. The second crew can schedule a deliberate progression from individual training to crew training to a mission element collective event and have the time to rehearse and refine their methodology. As we alternate these elements through training, we will be able to more deliberately incorporate lessons learned and maintain a broad range of skills rather than just focusing on the tasks immediately at hand.

The key for continuing to be ready to ***"Fight Tonight"*** is the striking of this balance between current operations and training that prepares us for future operations. While current operations can help refine our methodologies for specific tasks, we cannot let ourselves slip into the mindset that these missions prepare us for everything that will be asked of us in the future.

***FORT GEORGE G. MEADE, Md.***

*– Soldiers from the 781st Military Intelligence Battalion (Cyber), Vanguard, participated in a five kilometer battalion run to solidify their camaraderie and esprit de corps on April 6.*

*Following the 781st Military Intelligence Battalion run the Command Sergeant Major challenged each company to select their 'champion' and each competitor had to complete mountain climbers, a 50 yard sprint, and push-ups. (U.S. Army Photos)*

# 'Vanguard' Battalion hosts ceremony changing

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

***FORT GEORGE G. MEADE, Md.*** *-- Soldiers of the 781st Military Intelligence Battalion (MI BN) (Cyber) led by Master Sgt. Cory MacNeil, the commander of troops and the NCOIC (noncommissioned officer-in-charge) of one of the battalion's Cyber Protection Teams, stand in formation prior to a Change of Responsibility ceremony whereby Command Sgt. Maj. Cecil Reynolds relinquished his authority as the 'keeper of the colors' to Command Sgt. Major Jesse Potter, at McGill Training Center, March 7. (U.S. Army Photo)*

**FORT GEORGE G. MEADE, Md. –** Soldiers, Army Civilians, Family and friends said farewell to Command Sgt. Maj. Cecil Reynolds, the outgoing senior enlisted Soldier and 'keeper of the colors' for the 781st Military Intelligence Battalion (Vanguard), in a Change of Responsibility ceremony at McGill Training Center, March 7.

The 'keeper of the colors' is a position of honor and dates back to when Soldiers followed the cadence and instruction of the color guard, led by the color sergeant. In the heat of battle, the unit colors were always at the forefront of the formation. Today, the position of color sergeant is held by the senior most enlisted member of a command and they are known as 'the keeper of the colors.'

The more than 600 Soldiers and Civilians that comprise the 781st MI Battalion were represented at the ceremony by Soldiers from Headquarters and Headquarters Company, Alpha, Bravo, Charlie, and Delta companies, and the Cyber Solutions Development Detachment. According to the narrator, a large part of the battalion's Soldiers and Civilians could not take part in the ceremony as they were executing cyberspace operations in support of Army Cyber Command and the United States Cyber Command in the defense of our Nation.

The commander of troops for the ceremony was the NCOIC (noncommissioned officer-in-charge) of one of the battalion's National Cyber Protection Team, Master Sgt. Cory MacNeil, and the host was the commander of the 781st MI Battalion, Lt. Col. Justin Considine.

In his comments, Lt. Col. Considine remarked that Reynolds, in his two plus years as the Vanguard 7 (command sergeant major), was the embodiment of a Vanguard Soldier.

"You have protected this house…By knowing the shape of the Vanguard Soldiers and Civilians, by knowing their strengths, their heart, their attitude, their personalities, and their experiences," said Considine. "You have protected their health and

***FORT GEORGE G. MEADE, Md.*** *-- Command Sgt. Maj. Cecil Reynolds (right), the outgoing senior enlisted Soldier for the 781st MI BN (Cyber), relinquished his authority as the 'keeper of the colors' to Lt. Col. Justin Considine, the 781st MI BN commander, during a Change of Responsibility ceremony at McGill Training Center, March 7. (U.S. Army Photo)*

# the 'keeper of the colors'

***FORT GEORGE G. MEADE, Md.*** *-- Command Sgt. Major Jesse Potter (left), is the new senior enlisted Soldier for the 781st MI BN (Cyber) and assumes responsibility as the 'keeper of the colors' from Lt. Col. Justin Considine, the 781st MI BN commander, during a Change of Responsibility ceremony at McGill Training Center, March 7. (U.S. Army Photo)*

welfare, encouraged their holistic resilience, and ultimately increased the readiness and combat power of these warfighters, and left us all a little better than you found us…and that is ultimately your legacy."

The Reynolds family next assignment is with the 1st Information Operations Command (Land), Fort Belvoir, Virginia. Command Sgt. Maj. Reynolds will assume the mantle as the 1st IO Command senior enlisted Soldier and their "keeper of the colors" on April 2.

In his farewell remarks, Command Sgt. Maj. Reynolds talked about the battalion's accomplishments; however, he gave full credit to the Vanguard Soldiers and Civilians – past and present.

"Just remember every day is an opportunity, and in our business; people are a pacing item (the most critical aspect of an organization)," said Reynolds.

The incoming command sergeant major, and new 'keeper of the colors', is Command Sgt. Major Jesse Potter, who comes to the battalion from his previous assignment as the 780th MI Brigade operations sergeant major.

Command Sgt. Maj. Potter enlisted in the army as a chemical operations specialist in Jan. 1994, later reclassified to electronic warfare in 2009, and cyber operations in 2015 – the Army only recently approved the creation of a Cyber branch in September 2014.

"Successful succession is more than selecting someone with an appropriate skillset", said Considine. "It's about finding someone who is lock step with an organization's identity and purpose. That's why we call it succession and not replacement. There is continuity in vision. In the Vanguard, that vision is to be an elite cyberspace maneuver force, always out front…in the fight, using technology as a weapon system to defend the Nation. Sgt. Maj. Potter, we are excited to have you and your Family join the Vanguard team."


***FORT GEORGE G. MEADE, Md.*** *-- Soldiers, Army Civilians, Family and friends said farewell to Command Sgt. Maj. Cecil Reynolds, the outgoing senior enlisted Soldier and 'keeper of the colors' for the 781st MI BN (Vanguard), in a Change of Responsibility ceremony at McGill Training Center, March 7. (U.S. Army Photo)*

# Cyber Soldiers compete for honor to represent the Brigade at

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

***FORT GORDON, Ga. –*** *Sgt. Savannah Matelski, Company D, 781st Military Intelligence (MI) Battalion, simulates treating a casualty, which is an Army Warrior Task, as part of the 780th MI Brigade's Best Warrior Competition, April 23. (U.S. Army Photo)*

**FORT GORDON, Ga. –** There is an old Army axiom sergeants like to say when the weather turns bad: "If it's not raining, then we're not training."

Nothing could have been further from the truth for the first day of the 780th Military Intelligence (MI) Brigade (Cyber) Best Warrior Competition (BWC) which saw more than an inch of rain.

"Welcome to Georgia," stated one of the brigade BWC cadre members.

The competition, which took place April 23 through 25, was held to determine the organization's top warrior Soldier and noncommissioned officer (NCO), and those two champions will represent the brigade at the North Region U.S. Army Intelligence & Security Command (INSCOM) BWC in May.

The two Soldiers who braved the elements in the grueling three-day competition and will represent the brigade at the next BWC are: Spc. Alexander Musarra from Miami, and Sgt. Savannah Matelski, from Brandenburg, Kentucky. Spc. Musarra is currently assigned to Company B, 782nd MI Battalion (Cyber), headquartered at Fort Gordon, and is the brigade's top Soldier; and Sgt. Savannah Matelski, is assigned to Company D, 781st MI Battalion (Cyber), headquartered at Fort Meade, Maryland, and is the brigade's top NCO.

"I think it's a huge honor to represent the 780th MI Brigade, along with being part of the CPB – it is kind of like a dual-hatted honor," said Matelski. Although Matelski is assigned to the 780th MI Brigade, her team receives her operational requirements from the Cyber Protection Brigade (CPB). "I personally want to thank my leadership, including Staff Sgt. (Jeff) Newsome (her mentor), who have been very supportive of my training and everything, and my Family for getting me to where I am today."

Along with thanking his leadership and mentor, Staff Sgt, Aaron Bailey, Musarra credited the other competitors, specifically Spc. Francisco Ramos, Co. C, 781st MI Battalion, for challenging him throughout the competition.

"Moving forward means a lot because I know I put a lot of effort into this both before and during the competition," said Musarra. "But I am also grateful… to have the opportunity to move forward and maintain a determined, but humble perspective on the whole thing."

On day one of the brigade BWC, the first event started at 5:20 a.m. and the day did not end until 9 p.m. As with most BWC events, the competition started with an Army Physical Fitness Test. After the competitors performed personal hygiene and had a light breakfast,

# the Best Warrior Competition

they were right back at it. Other day-one events included: Army Warrior Tasks; a day and night land navigation course; M4A1 carbine rifle and military M9 9mm pistol familiarization; M4A1 zero and qualification; and an M4A1 Stress Shoot exercise.

During the Stress Shoot exercise competitors were given ten seconds to study a poster with four numbered targets. The Roman numeral on each target designated the number M4A1 rounds competitors would place into each target. The cadre informed competitors a ten-round magazine would be waiting for them at their firing point, and they were to lock and load that magazine once each competitor. After bring given the go signal, competitors ran 100 yards; completed ten burpees with a push-up; ran another 100 yards; completed ten squats; ran another 100 yards; completed ten eight-count push-ups; ran the last 50 yards back to their designated firing point; and fired at the targets. The event was timed, and the number of correctly hit targets, was also tallied.

"For day one, the toughest thing for me was the qualifying range. I didn't get a good zero, one that I was confident with from the beginning, so it kind of shook my confidence on the range," said Musarra. "The stress shoot was challenging as well. I've never done anything like that and I didn't know what to expect, but when it was over it was fun."

On day two of this year's brigade BWC, the competitors began their morning on a 12-mile road march with a 45-pound ruck. Soldiers then completed a written essay before going right into the Army Combat Readiness Test (ACRT) which included: as many leg tucks as they could perform, standing power throw, deadlift, T-pushup, and a shuttle run including two 25 meter sprints, a 90-pound sled pull and then a hand carry of two 40-pound kettle bells. The ACRT ended with a two-mile run, which after the road march was exceptionally grueling for each competitor.

"The toughest thing for me was the 12-mile ruck, because yesterday, during the land nav (navigation), rucking it with a 35-pound ruck, that was something that I hadn't done before," said Matelski. "We did about ten miles total, along with night land nav with a 30-pound ruck; and then to increase to 45-pounds, which was 15 pounds more than what I was used to – it was really difficult."

At the end of the second day, Command Sgt. Maj. James Krog, the senior enlisted leader for the 780th MI Brigade (Cyber), asked the competitors, "Two days of hell, but did you have fun?"

Krog stated the event organizers deliberately compressed the schedule of the competition to challenge the competitors after talking to last year's Soldier of the Year, Sgt. Johnny Long, who competed and was the champion at the brigade, North Region INSCOM, INSCOM, and U.S. Army Cyber Command BWC events.

"We purposely stacked all the physical events together," said Krog. "One, to see how much heart the competitors had, and two, to see what they need to focus on at the next level."

In addition to identifying the brigade's best warrior Soldier and NCO, Krog stated the competition sets these competitors apart from their peers.

"These Soldiers volunteered to do this, above and beyond what they do every day," said Krog. "The Army Best Warrior Competition not only builds esprit de corps, but it identifies those Soldiers who aspire to do greater things."


***FORT GORDON, Ga. –*** *Spc. Alexander Musarra, Company B, 782nd MI Battalion (Cyber), competes in the 12-mile road march while carrying a 45-pound ruck, on day two of this year's 780th Military Intelligence Brigade's Best Warrior Competition, April 24. (U.S. Army Photo)*

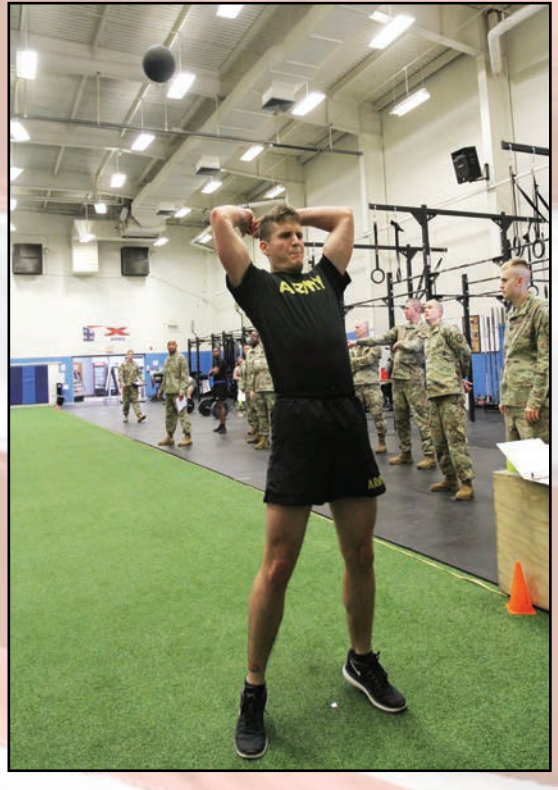
***FORT GORDON, Ga.*** *– Spc. Francisco Ramos, Company C, 781st Military Intelligence Battalion (MI BN) (Cyber), evaluates a casualty, an Army Warrior Task, on day one of the Brigade's Best Warrior Competition, April 23.*

***FORT GORDON, Ga.*** *– Sgt. Savannah Matelski, Company D, 781st MI BN (Cyber), is shown here firing her M4A1 carbine rifle during the qualification range which was an event on day one of the brigade's Best Warrior Competition, April 23.*

***FORT GORDON, Ga.*** *– Staff Sgt. Matthew Robinson, Company C, 782nd MI BN (Cyber), returns from the land navigation course on day one of the Brigade's Best Warrior Competition, April 23.*

***FORT GORDON, Ga.*** *– Spc. Alexander Musarra, Company B, 782nd MI BN (Cyber), from Miami, Florida, is shown here firing his M4A1 carbine rifle during the Stress Shoot Exercise which was an event on day one of the 780th MI Brigade's Best Warrior Competition, April 23.*


***FORT GORDON, Ga.*** *– Spc. Francisco Ramos (right), Co., 781st MI BN (Cyber), is shown here with his mentor, Staff Sgt. Scott Stappenbeck, as he competes in the 12-mile road march while carrying a 45-pound ruck, on day two of the Brigade's Best Warrior Competition, April 24.*




***FORT GORDON, Ga.*** *– Spc. Alexander Musarra, Co. B, 782nd MI BN (Cyber), competes in the standing power throw event during the Army Combat Readiness Test (ACRT) portion of the Brigade's Best Warrior Competition, April 24.*

***FORT GORDON, Ga.*** *– The Soldiers from the 780th MI Brigade who competed in this year's Brigade Best Warrior Competition are shown with their mentors (from left to right): Spc. Alexander Musarra, Company B, 782nd MI Battalion, was selected as the brigade's top Soldier; Musarra's mentor, Staff Sgt. Aaron Bailey; Staff Sgt. Matthew Robinson, Co. C, 782nd MI Battalion; Robinson's mentor, Staff Sgt. Sterling Robinson; Sgt. Savannah Matelski, Co. D, 781st MI Battalion, was selected as the brigade's top noncommissioned officer; Matelski's mentor, Staff Sgt. Jeff Newsome; Spc. Francisco Ramos, Co. C, 781st MI Battalion; and his mentor, Staff Sgt. Scott Stappenbeck.*


***FORT GORDON, Ga.*** *– Sgt. Savannah Matelski, Co. D, 781st MI BN (Cyber), took part in a 2-mile run as part the Army Combat Readiness Test (ACRT) portion of Brigade's Best Warrior Competition, April 24. The six-event ACRT was particularly challenging because competitors had recently completed a 12-mile road march earlier in the day.*

***U.S. Army Photos***

# Cyber Soldiers compete in the Best Warrior

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

*The Leonidas Trophy was awarded to the top Soldier and noncommissioned officer of the North Region INSCOM Best Warrior Competition.*

***FORT GEORGE G. MEADE, Md.*** *– Spc. Alexander Musarra (right), Company B, 782nd Military Intelligence (MI) Battalion (Cyber), 780th MI Brigade (Cyber), receives the Army Commendation Medal from Col. Rhett Cox, commander of the 704th MI Brigade, for being the top Soldier at the North Region Intelligence & Security Command (INSCOM) Best Warrior Competition award ceremony at Club Meade on May 11. (U.S. Army Photo)*

**FORT GEORGE G. MEADE, Md. –** As a Soldier, if you do not challenge yourself, you are just another Soldier.

Competing in an Army Best Warrior competition sets a Soldier apart from his peers; the experience, the camaraderie, the physical and mental toughness make every competitor a winner, regardless if he (or she) moves on to the next level.

Spc. Alexander Musarra, Company B, 782nd Military Intelligence (MI) Battalion (Cyber), 780th MI Brigade (Cyber), the top Soldier; and Staff Sgt. Melanie Wahl, 741st MI Battalion, 704th MI Brigade, the top noncommissioned officer, were crowned the champions of the 2018 North Region U.S. Army Intelligence and Security Command (INSCOM) Best Warrior Competition (BWC) in a ceremony at Club Meade, May 11.

Though she was not selected to move on, Sgt. Savannah Matelski, Company D, 781st Military Intelligence (MI) Battalion (Cyber), 780th MI Brigade (Cyber), enjoyed challenging herself alongside the other competitors.

"No regrets," said Matelski. "I would recommend the competition to my Soldiers because it tests their limits on other Army skills rather than always staying focused on our missions in cyber."

Matelski also said the competition identifies your strengths and weaknesses.

"Army Warrior Tasks and Battle Drills – those tend to be neglected in [cyber] units," said Matelski. "I'll bring those back to my company and train my Soldiers on that."

For Musarra, the BWC is an event in which he really enjoys participating.

"As hard and as grueling as it was, and I've been through three competitions, I'm hooked on it," said

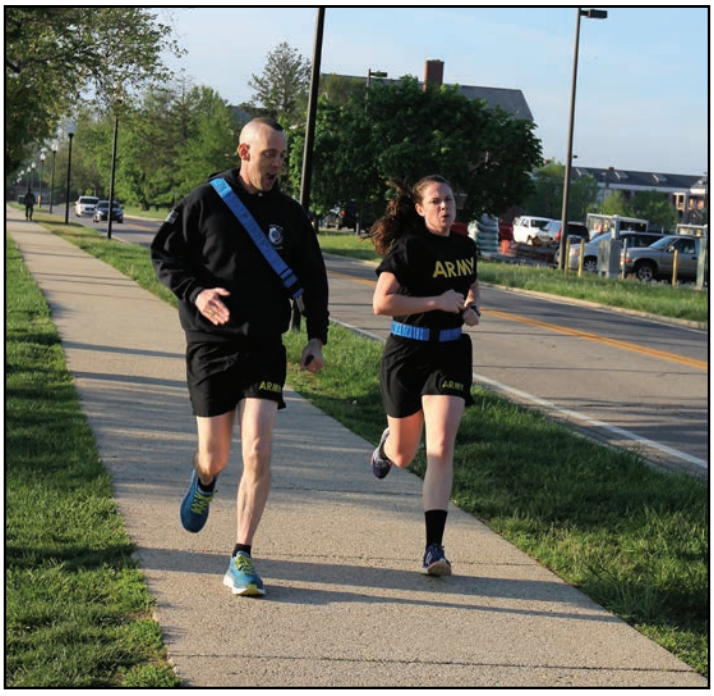
# Competition to challenge themselves

Musarra. "It's a yardstick to see how well you can do. You don't know what you are capable of until you are put into a competitive environment. It's not even about winning. I love these multi-events, multi-day competitions. You're shooting, running, rucking, assessing a casualty, land nav (navigation) – I can't get enough of it."

While Matelski's journey is over, Musarra will move forward to the INSCOM-level competition in June, and he comes away from the event better prepared for the next one.

"I did make some mistakes, but I'll never make them again," said Musarra. "Win or lose, I'm coming out of this a better Soldier."

***FORT GEORGE G. MEADE, Md.*** *– Sgt. Savannah Matelski, Company D, 781st Military Intelligence (MI) Battalion (Cyber), 780th MI Brigade (Cyber), receives a certificate of appreciation for having the highest board score during the North Region INSCOM Best Warrior Competition award ceremony at Club Meade on May 11. (U.S. Army Photo)*


***FORT GEORGE G. MEADE, Md.*** *– Day one of the North Region INSCOM Best Warrior Competition started out with the Army Physical Fitness Test on the Parade Field, May 7. Shown below are Spc. Alexander Musarra (left), and Sgt. Savannah Matelski.*

***FORT GEORGE G. MEADE, Md. –*** *Spc. Alexander Musarra answers questions posed by an INSCOM panel of command sergeants majors on day one of the North Region INSCOM Best Warrior Competition in the garrison headquarters, May 7. (U.S. Army Photo)*

***FORT A.P. HILL, Va. –*** *Spc. Alexander Musarra, Company B, 782nd Military Intelligence (MI) Battalion (Cyber), 780th MI Brigade (Cyber), fires his M4A1 carbine rifle at the qualification range on day two of the North Region INSCOM Best Warrior Competition, May 8. (U.S. Army Photo)*

***FORT A.P. HILL, Va. –*** *Spc. Alexander Musarra, Company B, 782nd Military Intelligence (MI) Battalion (Cyber), 780th MI Brigade (Cyber), fires his M9 9mm pistol during a stress shoot event on day three of the North Region INSCOM Best Warrior Competition, May 9. (U.S. Army Photo)*


***FORT A.P. HILL, Va. –*** *Sgt. Savannah Matelski, Company D, 781st Military Intelligence (MI) Battalion (Cyber), 780th MI Brigade (Cyber), finds her third check point during the day portion of the land navigation course on day two of the North Region INSCOM Best Warrior Competition, May 8. (U.S. Army Photo)*


***FORT A.P. HILL, Va. –*** *Sgt. Savannah Matelski, Company D, 781st Military Intelligence (MI) Battalion (Cyber), 780th MI Brigade (Cyber), competes in a timed 12-mile road march on day three of the North Region INSCOM Best Warrior Competition, May 9. (U.S. Army Photo)*

***FORT A.P. HILL, Va. –*** *Sgt. Savannah Matelski, Company D, 781st Military Intelligence (MI) Battalion (Cyber), 780th MI Brigade (Cyber), fires her M4A1 carbine rifle in the kneeling position as part of a stress shoot exercise on day three of the North Region INSCOM Best Warrior Competition, May 9. (U.S. Army Photo)*

***U.S. Army Photos***

# Transitioning from DCO to OCO – The Company

*By Capt. K. Lee Shelton, 106th Cyber Mission Team, 782nd Military Intelligence Battalion (Cyber)*

When I arrived at the Cyber Protection Brigade in 2014, there was little force structure, no computers, and no work space for Soldiers. We quickly task organized and got on our feet, developed a command structure, found office space, purchased equipment, and began training. We did what we had to do in order to accomplish the mission. After serving as team battle captain for two cyber guard exercises and one six-week Advance Cyber Training-Pilot mission and serving as Observer Controller-Trainer for one Cyber Flag exercise, I began to understand the DCO mission quite well and might even say that I became comfortable in my position.

After two years at the CPB, I completed the cyber captain's career course and transitioned into my follow-on assignment with the 782nd Military Intelligence (MI) Battalion. I had longed to engage in offensive operations against our enemies; however, soon after my arrival I realized I was far behind the learning curve. We used to say on the defensive side that our job was harder because "we had to be perfect all the time, and the offensive guys just had to get lucky once." But when faced with all of the policies, bureaucracy, and requirements that must be met in order to conduct an offensive operation, I realized that my assumptions of it being easier were totally false and that the cyber captain's career course had not effectively prepared me for a position in OCO. While the maneuver common core portion of the career course had helped me hone my planning skills, the cyber portion of the course was inadequate.

I wish I had known how offensive teams are structured, how they conduct missions, and what each part of the team does as it relates to the team as a whole. Prior to coming to 782nd, I had no exposure to the different types of offensive teams or their mission types. Guest speakers during the captain's career course gave us overview briefings, but we didn't get an in-depth understanding at all.

I also wish I had known much more about military intelligence operations and how it drives cyber offensive operations. Coming from the 25A Signal Officer world, I have an understanding of computer networks; but cyber is not signal. Cyber is also not just military intelligence, however, an understanding of military intelligence is required in order to know how the full circle of offensive cyber operations achieves mission success.

There is much debate in the cyber branch as to how a cyber force should be organized, how to train a cyber force, and whether or not a Cyber Warfare Officer should specialize in one field or generalize in all aspects of cyber warfare. As one of a small group of Soldiers that has seen both Offensive Cyber Operations (OCO) and Defensive Cyber Operations (DCO), and taking into account all of the things I have learned on both sides of the fence, there are three things I would change in our current cyber forces if given the chance. First, our cyber training and doctrine must be better established, and more effective. Second, Cyber Warfare officers need more experience writing orders and leading troops. And lastly, cyber leaders and Soldiers need to stay in place in order to learn and grow the force to maturity.

***Cyber training and doctrine must be better established, and more effective***

Army Chief of Staff General Mark A. Milley said, "…the first shots of the next actual war will likely be fired in cyberspace and likely with devastating effect" (Curthoys, 2016). Our current cyber training and doctrine is better than what we had four years ago, but it still does not meet the expectation of training our Soldiers to provide a "devastating effect" in cyberspace. The Cyber Force training and doctrine is still evolving. But we cannot wait on the school house to catch up. Everything we do in cyber must get faster. Until the training and doctrine is written, put in place, tested, and certified, we as company grade officers must play an active role in letting the leadership know what the ground truth is where the rubber meets the road. If we sit back and whine about how things are broken without doing anything to help fix them, we are doing a disservice to the future of the Army and the cyber force.

The question then becomes, do we, as the Army,

develop our own training and doctrine independent of the other armed services, despite the fact that Cyber Command is a joint command? I suggest that we lead the way and perfect a training and doctrine that works. When we started out in the Cyber Protection Brigade, what we had didn't work. We evolved and found things that did work.

***Cyber Warfare officers need experience writing orders and leading troops***

I suggest that we create an all-encompassing cyber basic officer leadership course (BOLC) which includes instruction on writing operations orders for cyber operations. There should be in-depth instruction on how exactly defensive teams and offensive teams conduct missions. A caveat with this is the fact that no two teams in the cyber force conduct mission in the same way, hence the need for standardization that starts at the school house. The course should also include exercises involving the planning and execution of major cyber defensive and offensive operations. I would also include all of the required training for every offensive and defensive work role. This would include getting the required accesses and clearances before leaving the school house. No need to show up at a new unit ready to fight unless I am qualified to start fighting. Lastly, the cyber BOLC should include a capstone exercise that involves planning and executing a team defensive mission, and then also an offensive mission.

Alternatively, I suggest we create a branch detail program that sends junior company grade officers to a maneuver career field for 3 years, and then bring them into the cyber career field through an immersive transition course. This will provide the operational experience an officer needs when supporting the maneuver forces, as well as help the officer lead and direct a cyber team. While at the Cyber Protection Brigade, my team and I was fortunate enough to attend a six-week training program called Advanced Cyber Training – Pilot (ACT-P). We were sequestered to Camp Dawson, West Virginia for multiple, grueling, on-net exercises that included three multi-day cyber guard type missions. Each mission was an average of ten days long and was separated by several days of cyber defense instruction taught by subject matter experts from the civilian cyber defense industry. We worked 12 to 14 hours a day, six days a week, and we learned more as a team than we ever would have learned individually. This type of immersion got us away from our daily distractions and forced us to depend on each other's strengths as well as help each other overcome our weaknesses. It helped us to understand that cyber is a team fight, and not just one super technical operator on a keyboard.

As an improvement to the cyber captain's career course, we need to have Military Decision-Making program (MDMP) instruction centered on cyber operations. The maneuver common core course is great to learn planning, but it does not provide effective, all-inclusive cyber operations planning for offensive and defensive cyber operations. The captain's course should also go more in-depth on the military intelligence aspect of cyber operations. A good place to start is Joint Publication 3-12(R), Cyberspace Operations (CO), dated February 5, 2013. Although the document is ancient in today's fast moving cyber world, it does give an overarching introduction of CO at the joint level. Many captains have not worked at the joint level and this will introduce them to a joint environment so they are better prepared for joint assignments. It also includes instruction about the relationship of Intelligence to CO. (Staff, 2013)

Technical training should still be included as necessary. Based on my experience, company grade officers need enough technical training in order to understand the effects of the actions of their Soldiers. You cannot make effective operational decisions without knowing what your Soldiers are capable of, and what the second and third order effects of their actions will likely be. Think of the Infantry officer. He knows the maximum effective range of all his weapon systems. He knows what he can kill with the weapons he has. The same is true for cyber officers. We need to know the effects of our systems and how they are employed.

*Continued on page 35*

# CyberPatriot is much more than a competition,

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

***BALTIMORE –*** *Sgt. Gregory Mills (left), a CyberPatriot mentor from Detachment Hawaii, 782nd Military Intelligence Battalion (Cyber), based out of Schofield Barracks, Hawaii, talks to JROTC Cadet Daniel Brink, a student from Leilehua High School in Wahiawa, Hawaii, about the CyberPatriot X Facebook Challenge, April 16. (U.S. Army Photo)*

**BALTIMORE –** In her remarks at the 2018 RSA conference in San Francisco, the Secretary of Homeland Security Kirstjen Nielsen described how she views the problem of cybersecurity, "We have a weakest link problem and the consequences affect us all."

According to the Leilehua High School CyberPatriot team that traveled here from Wahiawa, Hawaii, to compete in the CyberPatriot X National Finals competition at the Hyatt Regency Inner Harbor, April 15 to 18, the CyberPatriot program strengthens each participant by establishing a solid foundation for cyber defense – eliminating the weakest link by strengthening each of the six participating team members.

The CyberPatriot team from Leilehua High School, the Mules, consists of six Junior Reserve Officer's Training Corps (JROTC) cadets, their coach and a cadre of U.S. Army cyber Soldiers who are the team's mentors. The Mules are one of only 28 teams that were invited to the CyberPatriot X event out of the more than 5,500 teams registered to compete in the CyberPatriot program in 2017.

"These students are pioneers in our changing society, promoting responsible communication networks," said Sgt. Gregory Mills, a CyberPatriot mentor and the team's lead Windows instructor, from Detachment Hawaii, 782nd Military Intelligence Battalion (Cyber), based out of Schofield Barracks, Hawaii. "What really benefits us as a society is for our citizens to have this knowledge going forward to inoculate themselves from computer viruses, from malware, and from threats to our communication networks in the same way that you inoculate your children against viruses."

The Soldiers from Detachment Hawaii have been mentoring the students since last fall. They are all volunteers and spend countless hours after their work day, twice a week, to prepare the young people not only for the competition, but a future in cybersecurity.

"CyberPatriot is really good at giving the students the tools and skills they need to give back to society, whether that is in the private industry or if it is in the military or government," said Spc. Jacob Cochran, CyberPatriot mentor and the team's lead Linux instructor, from Detachment Hawaii, 782nd MI Battalion. "CyberPatriot is teaching these students the foundational knowledge they need to give back to society and protect our communication networks."

According to the mentors, the six competing team members have nine hosts they need to secure, along with the full network stack, during the CyberPatriot competition.

"The competition is primarily defensive. The participants' job is to secure their networks and to

# it strengthens US cyber defense

secure their hosts," said Spc. Evan Wittman, the lead CyberPatriot mentor from Detachment Hawaii, 782nd MI Battalion. "The difference between National Finals and all the previous competitions leading up to the finals is there is no active red team during the competitions leading up to the National Finals, but here, for the first time they'll have to actively deal with people trying to break into their network, deface their websites, and break their servers."

Wittman and the other U.S. Army mentors believe the CyberPatriot program instructs high school and middle school students to perform basic tasks in cyber defense, which will enable their ability to perform these tasks when they get into the workforce, regardless if they join the military.

"At a very basic level, CyberPatriot will provide them with a general understanding for Windows, Linux, and Cisco," said Wittman. "They will identify a pathway that they enjoy, and as they proceed further up in the competition, if they get to finals, they will have a lot of opportunities in front of them – internship offers and scholarship opportunities; and ultimately, that will contribute to the nation in some way, shape or form."

Lt. Col. (retired) Nicholas Spiridigliozzi, the Leilehua High School JROTC senior instructor and CyberPatriot team coach, believes that the CyberPatriot program not only gives the students a career path, but it is also a matter of national security.

"What the CyberPatriot program is doing is providing the future generation of cyber defense, security people, and leaders that will help keep this nation safe," said Spiridigliozzi. "We see it every day, the issues in cyberspace and cybersecurity, and it just continues to get worse and worse."

The CyberPatriot National Youth Education Program was created by the Air Force Association (AFA) to inspire K-12 students pursue careers in cybersecurity or other science, technology, engineering, and mathematics (STEM) disciplines that are critical to our nation's future.


***BALTIMORE –*** *The Leilehua High School, Junior Reserve Officers' Training Corps CyberPatriot team from Wahiawa, Hawaii, recently competed in the CyberPatriot X National Finals competition to test their cyber defense skills against the best high school teams in the country at the Hyatt Regency Inner Harbor, April 15 through 18.*

*The Leilehua Mules, the team name and school mascot, are one of only 28 teams invited to the event out of more than 5,500 schools that registered to compete in the Air Force Association's national youth cyber defense competition in 2017. To be invited, the team had to compete in multiple rounds of Online challenges, a state round and then excel in the semi-final round. (U.S. Army Photo)*

# CyberPatriot team from Hawaii looks towards

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

***BALTIMORE –*** *The Leilehua High School JROTC CyberPatriot team, the Mules, from Wahiawa, Hawaii, recently competed in the CyberPatriot X All Service Division at the Hyatt Regency in Inner Harbor, April 15 to 18. The team is joined by their active duty mentors based out of Schofield Barracks, Hawaii and are shown here from left to right: Lt. Col. (retired) Nicholas Spiridigliozzi, the JROTC senior instructor and CyberPatriot team coach; Bernie Skoch, CyberPatriot National Commissioner, Air Force Association; Sgt. Gregory Mills, a CyberPatriot mentor, Detachment Hawaii (Det. HI), 782nd Military Intelligence Battalion (Cyber); Cadet Jacob Huerta, a junior; Cadet Tyler McWilliams, a sophomore; Cadet Daniel Brink, a sophomore; Cadet Jarod Olive-Stalling, Jr., a junior; Cadet Christian Villarreal, a junior; Cadet McCain Compton, a sophomore; Spc. Evan Wittman, the lead mentor; and Spc. Jacob Cochran, both CyberPatriot mentors from Det. HI. (U.S. Army Photos)*

**BALTIMORE –** In his remarks at the 2018 RSA cyber security conference in San Francisco Tuesday, Microsoft President Brad Smith said, "We recognize that we live in a new world. We're living amidst a generation of new weapons, and where cyberspace has become the new battlefield."

If cyberspace has become the new battlefield, the high school and middle school students participating in the Air Force Association's CyberPatriot X National Finals competition at the Hyatt Regency Inner Harbor, April 15 through 18, are the next generation of cyber warriors.

The Leilehua High School, Junior Reserve Officers' Training Corps (JROTC) CyberPatriot team from Wahiawa, Hawaii, recently competed in the CyberPatriot X National Finals competition to test their cyber defense skills against the best high school teams in the country.

The Leilehua Mules, the team name and school mascot, are one of only 28 teams invited to the event out of more than 5,500 schools registered to compete in the Air Force Association's (AFA) national youth cyber defense competition in 2017. To be invited, the team had to compete in multiple rounds of Online challenges, a state round and then excel in the semi-final round.

"CyberPatriot is the premier national high school cyber defense competition in the country," said Lt. Col. (retired) Nicholas Spiridigliozzi, the Leilehua High School JROTC senior instructor and CyberPatriot team coach. "It is very competitive and more challenging since we started doing this in 2010. It has grown in the number of teams and also in complexity. The young people now are much more challenged than they were seven years ago which is a good thing in my mind."

Spiridigliozzi offered two bits of advice for other schools looking to be successful in the AFA CyberPatriot program.

"For any CyberPatriot program to be successful you have to have great mentors. You can have great students, motivated and dedicated students, but if they don't have the trainers than you are going to struggle,"

said Spiridigliozzi. "The mentors that we have here, and I've seen a lot of mentors, are definitely some of the best in the nation."

The mentors for the Leilehua High School JROTC CyberPatriot team are cyber-trained Soldiers from Detachment Hawaii, 782nd Military Intelligence Battalion (Cyber), based out of Schofield Barracks, Hawaii. The Soldiers are all volunteers who train the students in cybersecurity at least twice a week during the school year after their work day.

Additionally, Spiridigliozzi remarked that the support of the school principal is equally just as important.

"Principal Jason Nakamoto is a big force multiplier for the Leilehua JROTC CyberPatriot team," said Spiridigliozzi. "He supports everything that we do, is engaged with everything that we do, and provides the needed resources for us to be successful. Principal Nakamoto has played a critical role in our success"

For the six cadets from the Leilehua High School JROTC CyberPatriot team, the CyberPatriot program and competition has been an opportunity to achieve their future goals. Each of the students plans on attending college; however, their paths into the cybersecurity workforce vary.

Cadet Jacob Huerta, a junior and the team captain, aspires to be an aerospace engineer. His focus area during the competition was the security of the overall network and leading the Leilehua Mules CyberPatriot team. "My focus is on the networking portion, which is connecting a bunch of devices together so they can communicate," said Huerta. "I protect it and I can set up a defense so nothing can get into the area. I was trained to use Cisco Packet Tracer, which is a network simulation and visualization tool."

Cadet Christian Villarreal, a junior, wants to become a cyber defender for either the National Security Agency or the Air Force. He originally joined the program as an elective, but he soon realized he found cybersecurity very interesting. "Metasploit, a penetration testing software, helps a lot," said Villarreal. "It has a lot of problems that can easily be identified and helps you figure out different ways to fix them."

Cadet Jarod Olive-Stalling, Jr., a junior, wants to become a Naval officer and work in cybersecurity. His focus area has been serving as the Windows administrator. "The mentors are training me on how to make my system secure," said Olive-Stalling. "How to make sure all the passwords are protected, how to make sure my users and interfaces are good and there is no hacking involved."

Cadet Tyler McWilliams, a sophomore, wants to follow in his family's footsteps and join the Army. He plans on becoming a cybersecurity operations officer. His focus area is the Linux operating system, more commonly known as Ubuntu or the Debian. "I am learning to secure those different operating systems and to secure vulnerabilities," said McWilliams. "I eradicate malware and dangerous software that most people wouldn't know about."

Cadet McCain Compton, a sophomore, is thinking of joining the Air Force under the special forces' branch. His area of expertise is the bridge between Windows and Linux. "I am part of the defense," said Compton. "What I do is find vulnerabilities and things that do not fit the baseline of what a computer should be and I fix that."

Cadet Daniel Brink, a sophomore, is the only team member who doesn't want to start out in cybersecurity. His career aspiration is to join the U.S. Army and become an Armor officer. "I spend a lot of time on computers and I really wanted to learn how to basically watch over my own computer, and CyberPatriot really helps with that," said Brink.

However, Spiridigliozzi says that CyberPatriot is not just a competition. The program benefits the cyber workforce and ultimately the cybersecurity of the United States.

"CyberPatriot not only gives students a career path, but it's also a matter of national security," said Spiridigliozzi. "We must continue to 'grow' our young people in cybersecurity as it is a critical piece to the future of our nation."

*(U.S. Army Photos)*

## 780th Military Intelligence Brigade Operations

**Cyber Support to Corps and Below (CSCB)**

- Chief of Staff of the Army directed Cyber pilot (May 2014)
- Integration of Army and Agency cyber capabilities at the tactical level incorporating Cyber, Electronic Warfare and Information Operations

**Support to Contingency Operations**

- Title 10 (T10) Platform to support Cyber Operations
- Support to cyber capabilities to block extremist avenue to disseminate info
- Support to Joint Task Force-ARES
- Maintaining cyber presence in Area of Hostilities, U.S. Central Command, and U.S. Africa Command

**Development Operations**

- Integration of Software/Hardware Development, Testing and Operations to rapidly produce cyber tools in support of current operations
- Continuous Development Operations (builds and maintains tool sets)
- Quick Reaction Capability Development (responds to missions with new tools)


## 780th MI Brigade Mission Statement:

**The 780th Military Intelligence Brigade conducts signals intelligence and cyberspace operations to create operational effects in and through the cyberspace domain to gain and maintain freedom of action required to support the Army and Joint requirements while denying the same to our adversaries.**

***"Everywhere and Always…In the Fight!"***


## Cyber Mission Force

- **National Mission Team/National Support Team – Defend the Nation; conducts global cyberspace operations to deter, disrupt, and defeat adversary operations in order to defend US critical infrastructure and key resources.**
- **Combat Mission Team/ Combat Support Team – Develop and employ offensive cyberspace capability to achieve or directly support Combatant Command objectives.**
- **CPT/Incident Response – Cyber Protection Teams remediate foreign threats local and foreign networks; currently supporting NSA capability remediation efforts**

## 780th Military Intelligence Brigade (Cyber) Milestones from June 2016 to June 2018

***Led the Nation's effort to complete the build of the Army's Offensive Cyber Mission Force***

- Brought all 21 of the brigade's cyber mission teams to full operational capability -- the first element of any of the Services to meet this milestone achievement

***Maintained and fostered command relationships with U.S. Army Cyber Command, U.S. Army Intelligence and Security Command, the Cyber National Mission Force Headquarters, and multiple Joint Forces Headquarters – Cyber across multiple Services and Joint elements***

- Executed operations with tactical, operational, and strategic impacts;
- Supported four different Combatant Commands; and
- Supported requirements from Fort Meade Garrison and Fort Gordon Garrison

***Established and expanded two Joint Mission Operation Centers from which offensive cyberspace operations are conducted by not only the brigade, but sister-Service cyber teams as well***

- These two locations doubled the capacity to conduct operations by teams of the brigade and across the Cyber Mission Force (CMF)

- In June 2016, the brigade conducted one to two operations per month. As a result of the expansion there are daily operations that occur 24/7

***Integrated the largest Army National Guard (ARNG) mobilization (TF Echo) ever for USCC***

- Seamless changeover between two ARNG formations whereby one cyber battalion transitioned with another to continue the Task Force Echo cyberspace mission

***Established Cyber Solutions Development (CSD) Detachment and consolidated developers***

- Formed to consolidate previously-dispersed cyberspace tool developers, and focus efforts to build solutions for both the CMF, and Army-specific cyberspace needs

***Trained over 100 Developers and initiated a Job Qualification Requirement (JQR) process to test and advance capabilities***

***Grew the pool of Operators by partnering and instructing an Army Operator Course at the Cyber Center of Excellence (CCOE)***

***Informed the Fiscal Year 2019 Cyber Warfare Support Battalion build through Cyber/Electro-Magnetic Activities (CEMA) Support to Corps and Below (CSCB) efforts***

- Executed support at four National Training Center rotations, providing fully integrated offensive elements to "expeditionary cyber teams" embedded with the rotational unit during both home-station training and during the training rotation
- Built and developed capability to the current battlefields

***Improved team and staff procedures resulting in consistently higher performance***

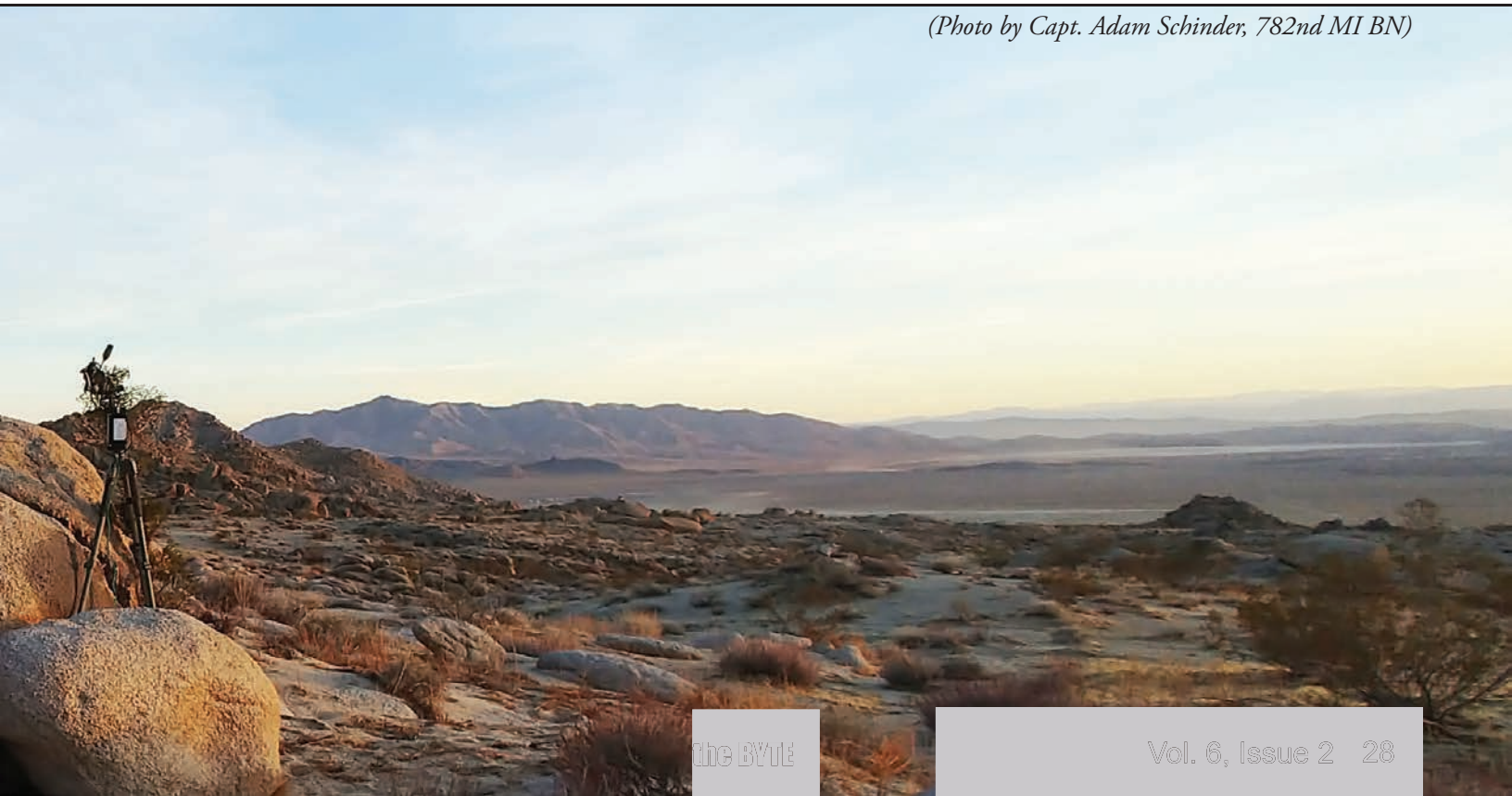
***Through Assignment Incentive Pay (AIP) / Special Duty Assignment Pay (SDAP), recognized and rewarded our advancing/improving population***

***Contributed greatly to our Sister Services and Higher Headquarters as part of the Cyber Enterprise***

***Kept the Army's leadership informed of our progress toward manning and training our cyberspace operations professionals to execute missions globally.***

- Articulated a readiness model for offensive cyberspace operations forces;
- Provided the clear vision that forces our Army to look at our offensive cyber teams as they would any other maneuver force;
- Established a standard of cyber firing crews with minimum manning and training requirements; and
- Clearly and accurately communicated the level of readiness defined by the number of crews trained and available to execute offensive cyberspace operations.

*(Photo by Capt. Adam Schinder, 782nd MI BN)*



# Task Force Echo II: Army National Guard Cyber

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

***FORT GEORGE G. MEADE, Md.*** *– The Soldiers of Task Force Echo, an Army National Guard (ARNG) comprised of more than 140 Soldiers from seven states, have completed more 38,000 hours of technical training and supported more than 1,500 U.S. Army Cyber Command and U.S. Cyber Command missions during their year-long mobilization. Because of their success, the Department of Defense has extended the TFE mission and will transition the current group of ARNG Soldiers with a new team of cyber warriors. (Photo by Schatz Strategy Group, Citizen Soldier magazine)*

**FORT GEORGE G. MEADE, Md –** The 780th Military Intelligence (MI) Brigade (Cyber) hosted an unprecedented transition of authority (TOA) ceremony between two Army National Guard (ARNG) formations whereby one cyber battalion transitioned with another to continue the Task Force Echo cyberspace mission, on a field near the brigade headquarters, April 19.

For the past year Task Force Echo (TFE) has worked with the 780th MI Brigade to conduct cyberspace operations in support of U.S. Cyber Command (USCYBERCOM) and the Cyber National Mission Force. The Task Force is aligned under the 780th MI Brigade, which falls under the operational control of U.S. Army Cyber Command (ARCYBER).

The outgoing TFE formation, the 123rd Cyber Protection Battalion (CPB), ARNG, was comprised of more than 140 Soldiers from seven states – California, Georgia, Indiana, Ohio, Michigan, Utah and Virginia.

The second iteration of TFE consists of ARNG Soldiers assigned to TFE 125th CPB, and these cyber warriors hail from Louisiana, Mississippi, New Jersey, New York, South Carolina, Texas, and Utah.

"Task Force Echo is an opportunity not only for the nation, but for the National Guard to step up and meet an ever growing challenge, that is a worldwide challenge," said Maj. Gen. R. Van McCarty, the Assistant Adjutant General – Army, South Carolina National Guard. "We see it every day, the potential impacts that we face in the cyber arena. Having young Soldiers that are trained and prepared to help meet those challenges is important."

The TFE mobilization is historic in that it marks the first ARNG task force mobilization of this size to support USCYBERCOM operations full time, and is a testament to the Army's commitment to the Total

***FORT GEORGE G. MEADE, Md.*** *– The 780th Military Intelligence ceremony between two Army National Guard formations whereby one Echo cyberspace mission, on a field near the brigade headquarters. (U.S.*

# Task Force Completes Transition

Force in defense of networks against the Nation's adversaries.

In the past year, the Soldiers of TFE 123rd CPB have completed more than 38,000 hours of technical training and supported more than 1,500 ARCYBER and USCYBERCOM missions. As a result of their proven success the Department of Defense extended the TFE mission, which resulted in the transition of the current formation of ARNG Soldiers with a new team of cyber warriors.

"(On) the 15th of March, the Secretary of Defense approved the extension – the establishment of the next iteration of Task Force Echo. It has never been done in that fashion before…never happened for a CONUS-based (Continental U.S.) unit," said Brig. Gen. JP McGee, the deputy commanding general of operations for U.S. Army Cyber Command. "When we properly articulated the role you (TFE) play…he understood the unique contributions of this organization."

Col. Dave Branch, commander of the 780th MI Brigade, summed up the accomplishments of the 123rd CPB and the importance of the TFE mission at the TOA event.

*Brigade (Cyber) hosted an unprecedented transition of authority (TOA) cyber battalion transitioned with another to continue the Task Force Army Photo)*

"Task Force Echo relies on Soldiers with diverse technical backgrounds. They come with the extensive experience that only comes from working in defensive cyberspace positions throughout the private sector and in the completion of the extensive training required to be a cyber warrior," said Branch. "During a recent awards ceremony, Brig. Gen. JP McGee made mention of how important it would be for the departing Soldiers of Task Force Echo to take back with them, all of the valuable lessons learned from their time here at Fort Meade. I second that sentiment, for it is only through continuous collaboration on the singular purpose of protecting our Nation, that we will ultimately prevail against those who would seek to do us harm."

The incoming and outgoing task forces are part of the 91st Cyber Brigade. The 91st Cyber Brigade is the Army National Guard's first and only cyber brigade and first unfurled its colors in September 2017. According to their mission statement, the brigade provides training, readiness and oversight of all ARNG Cyber Protection Battalions in order to provide ready, fully resourced, and proficient forces capable of conducting cyberspace operations in support of state and federal requirements. The brigade, comprised of Soldiers in thirty states, conducts cyberspace and information operations as authorized or directed to ensure freedom of action in and through cyberspace and the information environment and to deny the same to any adversary.

Col. Adam Volant, the outgoing TFE 123rd CPB commander, will command the 91st Cyber Brigade, and along with the other departing Soldiers of the first iteration of TFE, will form the nucleus of state assigned cyber protection teams and fall under the newly activated ARNG unit based out of Bowling Green, Virginia.

# Task Force Echo II: A continued Unity of Effort in

*By Maj. Mike Lass, S3 (operations), Task Force Echo II*


*FORT GEORGE G. MEADE, Md. – Task Force Echo (TFE) 125th Cyber Protection Battalion, Army National Guard (ARNG), is commanded by Lt. Col. Linda Riedel, and the senior enlisted leader is Command Sgt. Maj. William Kyzer III. The second iteration of TFE consists of ARNG Soldiers assigned to TFE 125th CPB, and these cyber warriors hail from Louisiana, Mississippi, New Jersey, New York, South Carolina, Texas, and Utah. (U.S. Army Photo)*

**FORT GEORGE G. MEADE, Md. –** The transition of authority between Army National Guard (ARNG) Soldiers assigned to Task Force Echo (first rotation) and Task Force Echo (second rotation), on April 19 was more than just another ceremony – it demonstrates a continued unity of effort in cyber operations.

The recently assigned Soldiers of the second iteration of Task Force Echo come from the 125th Cyber Protection Battalion, ARNG, and seamlessly continue the U.S. Army Cyber Command (ARCYBER) cyberspace mission.

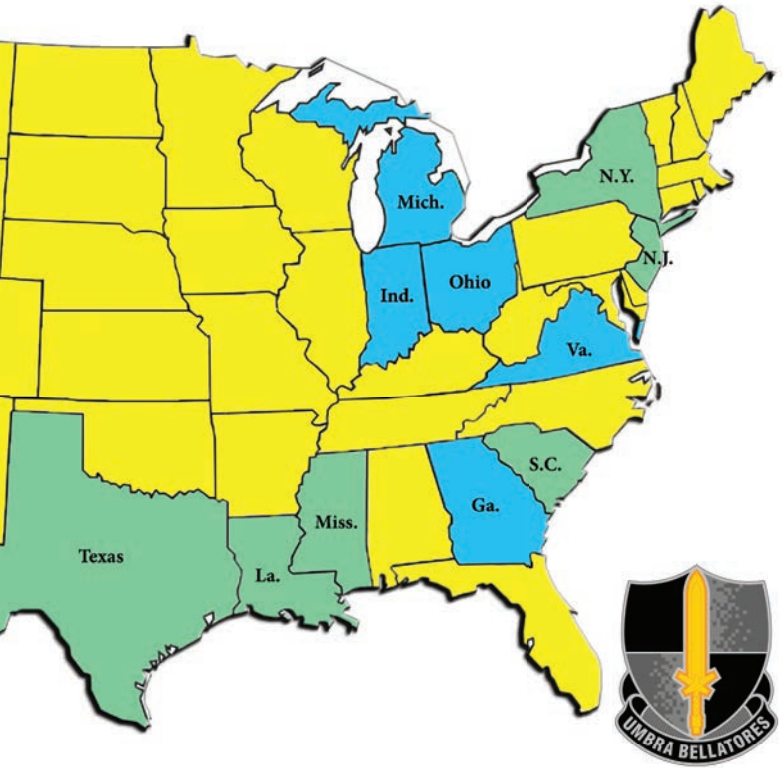
While serving on Active Duty, National Guard and Reserve units frequently train, deploy, and serve side-by-side, as seen in this blended formation. The event marks the first ARNG Task Force mobilization under the newly activated 91st Cyber Brigade, the ARNG's first and only Cyber Brigade. This rotation will continue to provide critical support to U.S. Cyber Command (USCYBERCOM), enabling cyberspace operations.

"The Citizen Soldiers of Task Force Echo come from strong academic and private sector backgrounds," said Lt. Col. Linda Riedel, incoming Task Force Commander. "We are a true group of diverse cyber professionals. My Soldiers work for the government, major defense companies and all areas of critical infrastructure within the States. They work for banks, power companies, law enforcement, colleges, and more. We understand the importance of collaboration and building partnerships."

The incoming Task Force is comprised of more than 150 Soldiers from various branches across the country to support the Cyber Mission Force. "When we got the call to support the cyber mission force, in less than five months the Battalion was stood up, activated and ready," said Riedel.

These Soldiers join teammates from across the Services who are already at work and on mission supporting USCYBERCOM and ARCYBER. They will operate

# cyber operations




under the 780th Military Intelligence Brigade (Cyber), an active duty Army organization, to engineer, install, operate, and maintain critical networks for USCYBERCOM.

The completion of Task Force Echo training and mission support is significant. They represent a vital part of the Army's Total Force, defending our networks against an ever-growing list of adversaries. The incoming Task Force will assume the critical mission of supporting the Joint Cyber Mission Force, a tremendous responsibility with an incredible legacy built by their predecessors.

"Our Soldiers get a chance to gain exposure in an environment they've never operated in before. It's a professional opportunity they will be able to build on with their employers within the States," Riedel said. "Military cyber operations is a very different and complex space. It takes a well-rounded Soldier, and a team effort to try and make sense of it all. That is what the Guard brings to the fight."

# Breakfast at M&T

***BALTIMORE –*** *Soldiers, Army Civilians, and their Family members from the 780th Military Intelligence (MI) Brigade's Headquarters & Headquarters Company, and Echo Company, 782nd MI Battalion, got together for some physical fitness, football, tailgating, and fun at the Baltimore Raven's M & T Bank Stadium, March 30. We wish to extend our sincerest gratitude to the Baltimore Ravens and the folks at the M & T Bank Stadium for their generosity in hosting us. It was truly a memorable occasion. (U.S. Army Photos)*

# Photo Page: PT at Raven's M&T Bank Stadium

***BALTIMORE** – Soldiers, Army Civilians, and their Family members from the 780th Military Intelligence Company, 782nd MI Battalion, got together for some physical fitness, football, tailgating, and fun at the our sincerest gratitude to the Baltimore Ravens and the M & T Bank Stadium staff for their generosity in (U.S. Army Photos)*

*Brigade's Headquarters and Headquarters Company, and Echo Raven's M & T Bank Stadium, March 30. We wish to extend hosting us. It was truly a memorable occasion.*



# DCO to OCO (cont.)

*Continued from page 20*

***Cyber leaders and Soldiers need to stay in place in order to learn and grow the force to maturity***

I know I may get flogged in the parking lot by my peers for suggesting this, but most of the Soldiers we have on both sides of the cyber domain right now are those that began building the force from the ground up. There are some starting to transition, but the force is not yet mature. Both OCO and DCO are still perfecting their process and procedures on how they conduct operations. Removing the subject matter experts during this time of maturation could be crippling to some units. How long do we leave them there? That depends on how fast the training pipeline and TRADOC can catch up. It could be several more years.

In my experience on the DCO side, most of the missions were fast-paced incident responses, and the execution of a mission after given the order to go could be less than 48 hours. The OCO target development process is much longer and drawn out and execution of a mission after identifying a target could be months. Understanding this process and learning how the intelligence drives the OCO team has been a challenge, but due to the good SME's on my team I have been able to overcome the challenge. However, there are very few SMEs who actually have time to train me up and get me smart on OCO. Those that can, are extremely busy in the fight, and some of them are on orders for PCS. If the SME's are moved from their current operational role, their next assignment should be as an instructor at the school house or in a position to influence the writing of policy and doctrine on cyber training.

In conclusion I would offer some advice to my fellow company grade officers. We are forging a new branch, there will be many growing pains. Do not get discouraged. Seek out the training you need from wherever you can. It is very tempting to follow the lure of a higher paycheck at a civilian company, but the Army and your country does need you. I am here because I am a patriot and I am passionate about this fight. Be patient and keep forging ahead. You are the future Field Grade and General Officers of cyber. Be proud of the work you have done and Stay "…In the Fight!"

***Works Cited***

*Curthoys, K. (2016, October). New Commander Takes Lead at Army Cyber Command. Retrieved from Army Times: https://www.armytimes.com/news/your-army/2016/10/14/new-commander-takes-lead-at-army-cyber-command/*

*Staff, J. C. (2013). Joint Publication 3-12(R), Cyberspace Operations. Washington DC: Joint Chiefs of Staff.*

# 782d MI BN CDR (cont.)

*Continued from page 4*

The three-day exercise included a road march, and setting up and conducting cyber operations from an observation post. The exercise was a success and an event to build upon.

The Battalion ran both the battalion-level and then the Brigade's Best Warrior Competitions. The winners from the Battalion included: Staff Sgt. Matthew Robinson and Spc. Alexander Musarra. Spc. Musarra subsequently won the Brigade and the North Region Intelligence & Security Command (INSCOM) Best Warrior Competition in the Soldier category and will represent the region at Intelligence and Security Command competition in mid-June.

In closing, the Battalion is fully engaged. We conduct the operational missions we are required to, but we also do so much more. Our staff provides world class service, our companies execute excellent training, and our people volunteer on post and in our community. The Battalion is and remains "Everywhere and Always…In the Fight!"

***"Cyber Legion...Silent Victory!"***

# 781st MI BN CDR (cont.)

*Continued from page 3*

We lack depth in training. For every 50 fully-trained and fully-qualified (FT/FQ) individuals leaving the unit after 12-24 months actually on mission, we receive only five FT/FQ gains, while at the same time we recognize that the current work role training pipelines we are required to follow are inefficient and ineffective at producing experts, which is a questionable expectation in itself since experience counts for so much in this domain.

We lack depth in equipping. We are still fielding the initial tranche of basic kit to our forces and therefore lack redundancy or separate training kits to prepare our crews for real-world operations. Infrastructure procurement is nascent, time-consuming, and high-maintenance while Continuing Resolutions (CR) and emergent requirements hamper budget forecasting.

And yet despite these challenges, we continue to deliver above and beyond the call of duty, leading all other Services in our impact to the Mission and to the Force. We delivered nine FOC teams one year ahead of schedule. We delivered the CSD. We delivered a re-purposed, expeditionary Shadow company. We delivered our Battalion to a new state-of-the-art facility. We delivered each company command post to new classified spaces. We delivered the highest retention rates, medical readiness rates, deployability rates, and Civilian strength rates in the unit's history. The list of significant contributions and accomplishments goes on and on.

We did all of this because we will never accept defeat or failure. We do not say 'no'. We leave it better than we found it.

On the other hand, to sustain this excellence, we must prioritize and we must accept risk "somewhere."

So as I prepare to relinquish command of the Vanguard Battalion to Lt. Col. Nadine Nally, a fantastic leader and long-time member of the 780th MI Brigade, I leave you with the following "deliverables":

Priority #1: Deliver a sustainable, unified mission command framework.

Priority #2: Deliver a sustainable force structure.

Priority #3: Deliver a sustainable readiness model.

It has been the most humbling and rewarding experience of my career to be your commander. Thank you for your Service and for your Sacrifice. I look forward to seeing what you deliver next.

***"Vanguard! When Others Cannot!"***

***"Everywhere and Always…In the Fight!"***

***FORT GEORGE G. MEADE, Md.*** *– While other brigade Soldiers look on, Col. Dave Branch, commander of the 780th Military Intelligence Brigade (Cyber), ensures Russ Strickler, Brigade SPO, maintains his form when 'knocking out' push-ups after a Fort George G. Meade Post Run. (U.S. Army Photo)*

# The 780th MI BDE continues a legacy of military operational innovation and development started by General Dwight D. Eisenhower and General George S. Patton....on the same spot at Fort Meade

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

Believe it or not, members of the 780th Military Intelligence Brigade (MI BDE) have something in common with General Dwight D. Eisenhower and General George S. Patton.

The 780th MI BDE Brigade headquarters at Fort Meade just so happens to sit on the same ground where Generals Eisenhower and Patton led the U.S. Army Tank Corps and Tank School over 90 years ago.

Between World War I and World War II, these two officers worked together to develop new U.S. doctrine in Tank warfare. Their new doctrine was based on developing faster tanks with more firepower that could quickly overwhelm and surprise enemy defenses during offensive operations. Working with tanks was often dangerous, and the two Tank Corps officers nearly lost their lives during a training event in which a tank cable snapped and whipped just 6 inches above their heads.

Had these two officers been killed during that training mishap on Fort Meade, the decisive Allied victory in World War II (just two decades later) may have been placed in jeopardy. During World War II, General Eisenhower was appointed as the Supreme Allied Commander in the European Theater and planned the successful D-Day invasion of Normandy France on June 6, 1944. Also during World War II, General Patton commanded the Third Army in Europe, responsible for coming to the aid of surrounded U.S. units at the battle of the Bulge (Germany's last major offensive).

Today, members of the 780th MI BDE are developing innovated methods in cyber operations with the same military operational goals as Generals Eisenhower and Patton pursued with tank warfare. Just like tank doctrine, cyber doctrine adds a new dynamic to the modern battlefield that can quickly overwhelm and surprise potential enemies. Tank warfare was vital for the Allied victory in World War II and it is very likely Cyber operations are just as vital for future potential conflicts. Like Generals Eisenhower and Patton did so over 90 years ago, the 780th continues to develop methods to keep our nation ***"Everywhere and Always in the Fight!"***

*Tank Corps photo taken at Camp Meade in 1921. Major George S. Patton is circled on the left and Captain Dwight D. Eisenhower is circled on the right. This photo appears in Stars and Stripes on line article "Tanks: from novelty to necessity in 100 years." (Photo courtesy Don Moriarty/Red Davis Library archives).*

# Catches of the day

*Story and photo by Lisa Rhodes, Fort Meade Soundoff!*

*Mark VIII tanks on maneuvers at Camp Meade (pictures provided courtesy of the Fort Meade Museum)*

***Sources:***

- *US Army Center of Military History at https://history.army.mil*
- *Eisenhower Leadership website at https://eisenhowersleadership.com/2012/10/31/eisenhowersleadership-patton-and-inn/*
- *Stars and Stripes article at "Tanks: from novelty to necessity in 100 years" @ http://media.stripes.com/i/tanks/*
- *Fort George G Meade museum website at http://www.ftmeade.army.mil/Museum/pages/Museum_Timeline_BTW.html*

**FORT GEORGE G. MEADE, Md. –** More than 50 families cast their lines on the banks of Burba Lake for sunfish, rainbow trout and largemouth bass during Fort Meade's Spring Youth Fishing Rodeo, April 28.

The free, five-hour event was co- sponsored by the Directorate of Family and Morale, Welfare and Recreation and the Meade Rod & Gun Club. More than 90 children competed in the fishing rodeo, which has also been held in the fall. Ribbons were awarded for the largest fish in each age category: 3 to 6; 7 to 11; and 12 to 15. All the young fishermen got to keep their catch.

The top prize went to 11-year-old Ethan Lasiter, son of Maj. Nolan Lasiter, the brigade S4, of Potomac Place, who caught the largest fish of the day — a golden rainbow carp, weighing 9.5 pounds. Ethan won first place for his age category and for the largest fish overall.

# SAAPM: Sexual Assault Awareness Prevention Month

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

April is Sexual Assault Awareness and Prevention Month (SAAPM). A lot of awareness activities were planned on the installation throughout the month, culminating in the Annual Amazing Race.

Teams started and ended on the Fort Meade Parade Field and navigated through six stations located throughout the garrison. Each station tested the knowledge and abilities of each eight-person team with activities such as "drunk" corn hole toss and a Sexual Assault Prevention and Response (SAPR) Minefield.

***FORT GEORGE G. MEADE, Md. –*** *This is the third year the 780th Military Intelligence (MI) Brigade has participated in the Amazing Race with two teams – one from the 781st MI Battalion and one from Headquarters & Headquarters Company, 780th MI Brigade, and Echo Company, 782nd MI Battalion. (U.S. Army Photo by Spc. Jordan Buck, 55th Combat Camera)*

"April is Sexual Assault Awareness and Prevention Month so the booth was set up to call attention to sexual harassment and sexual assault awareness," said Kimberly Henne, The Brigade SARC (Sexual Assault Response Coordinator), "We used the "What Would You Do?" Wheel to ask brigade members what they would do if put in certain situations. If they answered the question correctly, they won a prize. It also gave us the opportunity to educate people on a one-on-one basis. Everyone walks away a winner."


***FORT GEORGE G. MEADE, Md. –*** *Pictured here are some of the Brigade SHARP (Sexual Harassment/Assault Response and Prevention) team members, form left to right, Kimberly Henne, the Brigade SARC (Sexual Assault Response Coordinator), Sgt. 1st Class Donnette Irving, Staff Sgt. MarQuita Lacey, Sgt. 1st Class Raven Vargas, Staff Sgt. Kenya Guinn, and Sgt. 1sr Class Abraham Morales, who are all Brigade Victim Advocates. (U.S. Army Photo)*

***ELKRIDGE, Md. –*** *Glenda Demma (right), 781st MI Battalion, answers a question about sexual harassment and sexual assault after spinning the "What Would You Do?" Wheel at the 780th MI Brigade's Sexual Assault Awareness and Prevention Month booth, April 12. Staff Sgt. Charlie Talania, a battalion Victim Advocate and other volunteers set up the booth to increase awareness of sexual harassment and sexual assault in the Army and society." (U.S. Army Photo)*

# Merit, Fitness, and Capability: "In the Fight!"

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


Keeping Soldiers in the fight is a critical responsibility for leaders and commanders at all echelons. Unit personnel, Soldiers and Civilians alike, need to feel that they enter a work environment where they are judged based solely on their merit and capability. The goal of the Army's EO program is to promote a work environment free of unlawful discrimination and offensive behavior. While ultimately the Commander's program, it is everyone's responsibility to assist in creating a positive work atmosphere.

Discriminatory language or displaying of inappropriate materials undermines good order and discipline. The impact such behavior can have isn't always readily known, and how it affects each individual will be different in every scenario. Unit personnel should focus on how their language and actions could be seen by someone else, rather than by how they perceive them. In most cases, something that isn't offensive to you very well may be offensive to others. It can be hard in a social setting to make an on-the-spot correction, so use tact when someone says or does something that may not be appropriate. I encourage and challenge all leaders to set the example, and make those tough on-the-spot corrections.

With the summer PCS cycle starting to get in full swing, the Brigade is going to see a lot of personnel changes at all levels of Command. Newer Soldiers to the Army and the unit will be looking to Senior NCOs and Officers to see what right looks like. We all signed up swearing by an oath and promising to uphold the Army values. Using discriminatory language or displaying obscene or offensive material in the work place has no place in an Army where the values of Loyalty, Duty, Respect, Selfless Service, Honor, Integrity, and Personal Courage are ingrained and expected.

The best way to keep a Soldier in the fight is to make sure they are ready, able, and willing to come to work. Unit personnel should feel like they are regarded for what they can bring to the fight, rather than the color of their skin, their race, their gender, their sexual orientation, their chosen religion, or where they're from.

Keep an eye out for these upcoming EO observances at your local installation(s) in the coming months.

- Women's Equality Day: 26 August 2018
- National Hispanic Heritage Month: 15 September – 15 October 2018

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 comm: (301) 833-6412, bb: (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'm located in the Annex trailer at 310 Chamberlin Ave. on Fort Meade, MD. In addition, you can also contact your unit's Equal Opportunity Leader for assistance.

# Happiness AND Satisfaction

*By Staff Sgt. Patrick Grill, Religious Affairs Noncommissioned Officer, 780th Military Intelligence Brigade (Cyber)*

Do you suffer from feelings of dissatisfaction in some or all areas of your life? Join the club. You share this in common with over 200 million Americans if happiness can be considered synonymous with satisfaction.

Since the time of Aristotle, people have struggled to define and find the secret to happiness. It is the focus of whole religious movements and a quite a bit of modern research. However, given the number of people today that complain of unhappiness and dissatisfaction, it seems that all this attention has not yielded many results. Could it be that dissatisfaction is too deeply ingrained in our human nature to escape from?

Recently I visited my Grandfather who was born and lives in Malta Montana. Malta is in the northeastern Great Plains region. At 91 and as a farmer, my grandfather lived through the Great Depression, and the Great Plain Drought of the 20s and 30s that caused the Dust Bowl.

Always interested in family history I asked him about his life during the last century. He told me one thing which caught my attention. Even after living through the worst times of the 20th century it was during the better times in the 50s that his feeling of dissatisfaction led him to leave his farm and try and start a new life in the city. He later returned to the farm and regretted his costly adventure.

Something about his story struck a chord with me. I too, like most Americans, struggle with dissatisfaction. There is an underlying guilt in that as I have traveled, I see places and meet people who would be ecstatically happy to just have running water, shoes, or a little meat in their diets. I vividly remember the return from my first deployment and the great sense of thankfulness I had for my own bathroom and real plates and silverware. Those feelings quickly faded, however, and I returned to being unsatisfied with this or that. I think this is the human condition. As someone said, if you received everything you ever wanted today, tomorrow you would be making up a new list.

There can be a terrible cost to dissatisfaction. When our dissatisfaction in our job, marriage, possessions or what have you, leads us to make rash or unwise decisions, we often end up in a worse condition and even less satisfied that before. Some interesting statistics of divorce captures this well, while 50% of first marriages end in divorce, 67% of second marriages and 73% of third marriages subsequently end in divorce. I think this shows that the more we give in to our desires to find greener pastures, the easier it is to give up on our current endeavors or commitments. We find that the grass always looks greener of the next hill. If we accept that a certain amount of dissatisfaction is normal to the human experience we may find great blessing in sticking it out in our current situation.

# Household Safety


### Dialing Emergency Telephone Numbers

When an emergency occurs on the military installation, using a hardwired garrison phone line to dial 911 will route the emergency call to a military police desk or emergency operator. Hardwired or landline telephones provide for a more timely response from Garrison Military Police and Fire Department units.

When dialing 911 from a cell phone on a military installation, you will normally contact a 911 operator outside of the installation causing a delayed emergency response time. Please notify the 911 operator of your location and/or location of the emergency and the garrison you are calling from. If you need to make an emergency call using a cell phone, make direct contact with Fire Department or Military Police personnel by

# Household Safety

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

using the alternate direct dial emergency telephone numbers for the garrison you are calling from; these numbers are usually available on the garrison website. Program these numbers into your cell phone contacts list so they are readily available.

## Safety Devices Every Home Should Have.

### *Smoke Detectors*

One is definitely NOT enough! Every home should be equipped with smoke detectors on every level, particularly outside of sleeping areas.

Ensure that your smoke detectors are tested monthly and batteries are replaced twice a year. Change batteries when you change your clocks.

Encourage children to help test the smoke detectors. Familiarize them with the sounds of the alarm(s).

The National Fire Protection Association says that having a properly installed and maintained smoke detectors in your home more than doubles one's chances of surviving a fire and cuts the chances of dying in a reported fire in half.

### *Fire Extinguishers*

Keep an all-purpose (ABC type) fire extinguisher in your home. ABC type fire extinguishers use a multi-purpose dry chemical to fight against the most common fires that occur in homes and offices.

It is a good idea to keep fire extinguishers near the kitchen, furnace, garage, and anywhere else a fire may start. These extinguishers are affordable, life-saving equipment for your home. If you must use an extinguisher, make sure you have a clear way out in the event you cannot put out the fire. Post phone contacts list so they are readily available.

Make sure every able-bodied member of the Family is trained and familiar with the proper way to use the fire extinguishers.

A portable fire extinguisher can save lives and property by putting out a small fire or containing it until the fire department arrives; but portable extinguishers have limitations. Because fire grows and spreads so rapidly, the #1 priority for residents is to get out safely.

### *Carbon Monoxide Alarms*

Often called the invisible killer, Carbon Monoxide (CO) is an odorless, colorless gas created when fuels (such as gasoline, wood, coal, natural gas, propane, and oil) burn incompletely. In the home, heating and cooking equipment that burn fuel are potential sources of carbon monoxide. Vehicles or generators running in an attached garage can also produce dangerous levels of CO.

Carbon Monoxide enters the body through breathing. CO poisoning can be confused with flu symptoms, food poisoning and other illnesses. Some symptoms include shortness of breath, nausea, dizziness, light-headedness or headaches. High levels of CO can be fatal, causing death within minutes. According to the Centers for Disease Control and Prevention (CDC) more than 400 people die each year in the United States from CO poisoning. A Carbon Monoxide detector is the only way to know if the deadly gas is being omitted in your home and could save your life.

CO alarms should be installed in a central location outside each sleeping area and on every level of the home and in other locations where required by applicable laws, codes or standards. For the best protection, interconnect all CO alarms throughout the home. When one sounds, they all sound.

Follow the manufacturer's instructions for placement and mounting height. Choose a CO alarm that has the label of a recognized testing laboratory. Test CO alarms at least once a month; replace them according to the manufacturer's instructions. If the audible trouble signal sounds, check for low batteries. If the battery is low, replace it. If it still sounds, call the fire department. If the CO alarm sounds, immediately move to a fresh air location outdoors or by an open window or door. Make sure everyone inside the home is accounted for. Call for help from a fresh air location and stay there until emergency personnel arrive.

***References and Sources:***

*U.S. Army Installation Management Command/ Safety*

*National Fire Protection Association*
*Centers for Disease Control and Prevention*

# Why I Stay...In the Fight!

***FORT GEORGE G. MEADE, Md.*** *-- Staff Sgt. Ruben Reyna (right), Charlie Company, 781st Military Intelligence (MI) Battalion, reenlisted in the U.S. Army for an Indefinite Term under the Career Status Program. Capt. Mark Klink, administered the Oath of Reenlistment and presided over the ceremony. (Courtesy photos)*

**FORT GEORGE G. MEADE, Md. --** Staff Sgt. Ruben Reyna, from Whittier, Calif., a cyber planner assigned to Charlie Company, 44th National Mission Team, 781st Military Intelligence Battalion (Cyber), recently reenlisted in the U.S. Army and re-classed to 17C, cyber operations specialist, for an Indefinite Term under the Career Status Program.

Reyna joined the Army in June 2005 as an 11B, infantryman, and had re-classed to 35Q, cryptologic cyberspace intelligence collector/analyst, before coming to the 781st MI BN.

His wife, Caitlin Reyna, was at his reenlistment ceremony, along with Capt. Mark Klink, the reenlistment officiating officer.

*I enjoy my job, the Army is a great place if I am being honest. It provides people with the chance to do something that they would never have the opportunity to do on the outside.*

*With our mission and daily work being what they are, we get to see things on a global scale as they happen.*

*It is pretty awesome to see something on the news that you know about in advance or had a hand in directly.*

*The Cyber branch itself is fascinating because right now, from within the force, we get to watch it grow and see how it will develop. Nowhere else in the military does one have the chance to implement and direct change at this level.*

*It didn't take any real persuasion to reenlist. I knew I was going to because I do enjoy this line of work.*

*Right now I am right where I want to be. I have just re-classed to 17C, and I am happy with my Company and Team. There is a lot of respect and care given to members of both. This is probably the happiest that I and my family have been with a unit in the Army.*

*Staff Sgt. Ruben Reyna (left), Charlie Company, 781st Military Intelligence (MI) Battalion, shares a happy moment with his wife, Caitlin Reyna. (Courtesy photos)*

## 780th Military Intelligence Brigade Retention Team

**Senior Career Counselor**
**Master Sgt. Scott R. Morgan**
**Commercial: 301-833-6405**

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

**782nd Military Intelligence Battalion**
**Career Counselor**
**Sgt. 1st Class Michael Brothers**
**Commercial: 706-849-4789**

# Photos

**HHC/780th MI BDE fund raiser cookout**

***FORT GEORGE G. MEADE, Md.*** *– Soldiers and Army Civilians assigned to the 780th Military Intelligence Brigade (Cyber) supported a Headquarters and Headquarters Company, 780th MI BDE fund raiser cookout on April 12, whereby all the profits went to the company fund that offsets the Brigade Organizational Day, the Holiday Ball, and other unit events. (US Army Photos)*

**Spiritual Luncheon**

*FORT GEORGE G. MEADE, Md. – The Brigade Chaplain's office hosts a Spiritual Luncheon every Wednesday at 11:30 a.m. in the Brigade Annex. All Soldiers, Army Civilians and contractors are invited. (US Army Photo)*

# Clandestine Cold War unit honored at Fort Bragg

*By Drew Brooks, military editor, Fayetteville Observer*

*Note: Jim "Coop" Cooper, S3 / Cyber Training, 780th Military Intelligence Brigade, served with the 410th Special Forces Detachment in Berlin from 1989 to 1990, when the Berlin Wall came down, and his service is now a part of our American history. Please see the article below to read more about his story, because it is our story/ Also, there are more than a few Army civilians serving throughout with brigade with prior military service.*

Not quite a year after the Berlin Wall was opened, soldiers of the U.S. Army Physical Security Support Element-Berlin left the city without any fanfare.

The end of the wall, which had divided Berlin both physically and ideologically for decades, was a sign of the end of the Cold War. And the resulting "peace dividend" spelled the end for special units like the PSSE-B.

On the outside, the unit was tasked with providing security assessments of U.S. government buildings from South Africa to England. But its members had a secret.

The PSSE-B was actually the 410th Special Forces Detachment, a clandestine group of Green Berets tasked with unconventional warfare and counterterrorism, including a so-called "stay behind" mission in the event of a Soviet invasion.

The unit was the successor to a similar clandestine force, the 39th Special Forces Operational Detachment, often simply known as "Detachment A," which operated in Berlin from 1956 to 1984.

On Monday at Fort Bragg – 34 years after the 410th Special Forces Detachment formed and nearly 28 years since it was inactivated – members of the secretive unit gathered for the first time to celebrate their accomplishments and honor the unit's legacy.

The public acknowledgment of the unit was something its veterans, like retired Chief Warrant Officer 4 James Stejskal, never fathomed in the years immediately following the Cold War.

Stejskal authored a book about the two secretive units titled "Special Forces Berlin: Clandestine Cold War Operations of the U.S. Army's Elite, 1956 - 1990."

Like its predecessor, Detachment A, the 410th Special Forces Detachment was inactivated without ceremony, said Stejskal, who served with both units and later with the CIA before retiring.

On Monday, with dozens of veterans of the detachment in the audience, officials from U.S. Army Special Operations Command and the former unit unveiled a memorial stone, laid a wreath and officially furled the detachment colors.

Maj. Gen. James E. Kraft Jr., the deputy commanding general of USASOC, accepted the colors from retired Col. Mercer "Mac" Dorsey, the detachment's first commanding officer.

While handing off the colors, Kraft said Dorsey softly said just two words: "Mission accomplished."

"Those were pretty powerful words. Simple. Elegant. Definitive," Kraft said.

The general said the ceremony was a celebration of the unit's legacy, which builds on the greater legacy of Army special operations.


Working clandestinely behind enemy lines "requires an incredible amount of professionalism, dedication, dogged determination and a wiliness to sacrifice everything you care about in life for the mission at hand," Kraft said.

The 410th Special Forces Detachment embodied missions that continue to serve as the pillars of Army special operations, he said, including working with indigenous populations, precision targeting, developing a deep understanding and yielding influence in select parts of the world and countering terrorism.

The soldiers "embodied not only who we are but where we are going," Kraft said.

The memorial stone, which was covered with an East German flag before it was unveiled, joins more than 30 other stones honoring past and present special operations units in the Memorial Plaza.

The 410th Special Forces Detachment stone includes both of the unit's names, a map of a divided Berlin, two arrows crossing a dagger to symbolize Special Forces and a Trojan horse to symbolize the unit's unique mission.

The stone also includes the dates of the unit history and the words "In honor of the men who clandestinely served deep behind the Iron Curtain to safeguard our freedoms. They stayed until the job was finished and left before the devil knew they were ever there."

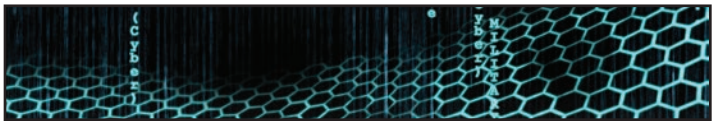
The idea for the memorial stone came in January 2014, Stejskal said. That's when a similar stone for Detachment A was unveiled in the Memorial Plaza.

Stejskal said the new stone helps to tell "the rest of the story."

Detachment A was inactivated following concerns with the unit's operational security, officials said.

Like their predecessors, soldiers of the 410th Special Forces Detachment sometimes dressed in civilian clothes and were tasked with fitting in with the styles, etiquette and other behaviors of those who lived in the divided city located 100 miles behind the Iron Curtain.

The unit was continuously on high alert and was called to respond to the hijacking of TWA 847 in 1985, the hijacking of the cruise ship MS Achille Lauro in 1985 and the La Belle Disco bombing in 1986.



# Cold War unit honored (cont.)

*(continued from the previous page)*

The soldiers constantly balanced their public mission to assess American diplomatic compounds with their classified missions to counter terrorism and prepare for all-out war.

In the event of World War III, the soldiers would be tasked with slipping behind the Soviet front lines to wreak havoc and target key facilities and infrastructure.

Like Detachment A – whose total historical roster numbers approximately 800 men – the 410th Special Forces Detachment was also a relatively small unit with a vast and important mission, Stejskal said. Its veterans likely number fewer than 250 soldiers.

"This is like a family reunion," he said as veterans posed for photographs after the ceremony.

Retired Sgt. Maj. Don Robblee, a former senior enlisted leader for the detachment, said the unit went through painstaking efforts to conceal its true purpose.

"Things aren't always what they seem," he said.

The unit only recruited the best to join its ranks, he said, pulling soldiers from the Army's most elite units.

The mission wasn't easy, Robblee added.

"But we done a pretty darn good job of it," he said. "We were on a great adventure."

Stejskal, reading a letter from Col. William Davis, the detachment's first executive officer who was unable to attend the ceremony, said the men of the detachment were extraordinary.

"The nature of what we did, with what we had, made our unit one that is legend," Davis wrote.

"It is very uncommon and frankly uncomfortable in our community to talk about being rare," he added. "We were very special indeed."

# Should I retweet this? What does the Hatch Act say?

*By Terry Wing, Federal News Radio*

***Should I retweet that political comment? When can I express my frustration with politicians on my Facebook page?***
Federal employees need to know the answers to those questions before posting their political views.

With local and national election season in full swing, the office that handles inquiries about the workings of the Hatch Act, the Office of Special Counsel, has clarified some of the nuances related to use of social media and published them on its website.

"We thought it'd be helpful to clarify and give some real world examples of what federal employees may do in the social media, in terms of staying on the right side of the Hatch Act," Special Counsel Henry Kerner told Federal Drive with Tom Temin.

"You can't tweet, retweet, share, or like a post or content that solicits political contributions at any time. And you can't engage in political activity via social media while on duty or in the workplace," said Turner.

Simply put, Kerner offers these bullet points for federal employees:

- Don't solicit or accept political contributions.
- Don't engage in political activity on duty or in your official capacity.
- Don't use your official position to promote or oppose candidates for partisan office.
- Don't run for partisan elective office as a federal employee.

Questions about drawing a line between political actions and the federal workplace are numerous.

Just this week, the OSC announced Counselor to the President Kellyanne Conway had violated the Hatch Act "by using authority or influence to interfere with or affect elections." It also found Federal Communications Commissioner Michael O'Rielly broke Hatch Act rules for what it ruled was a re-election pitch for President Donald Trump.

It's OSC's job to enforce the Hatch Act and ensure that federal programs are administered in a non-partisan fashion. As the agency's top administrator, Kerner suggested federal employees avoid mixing their First Amendment interests in political participation with your work. "As long as you keep those two separate, you should be OK," he said.

If you question whether your plans for participation in politics comply with the law, Kerner wants federal employees to know the Office of Special Council can provide guidance.

"We provide advisory opinions, thousands of them, in fact," Kerner said. "We have a website where social media guidance is very active, with a lot of really good, clear examples of what's allowed and what's not."

Hatch Act through the years

The Act has evolved since 1939, when Sen. Carl Hatch of New Mexico offered the legislation to protest of the political involvement of federal employees in primaries and general elections. The original measure focused on the misuse of official authority or influence, and the misuse of workplace and official duties.

Reform amendments to the law in 1993 relaxed the rules to allow federal employees permission to work on partisan campaigns, but only while off-duty,

More changes came when President Barack Obama signed the Hatch Act Modernization Act of 2012. It modified penalties to allow for disciplinary actions in addition to removal for federal employee, and allowed most state and local government employees to run for partisan political office.

What's less known about the Hatch Act is that it protects federal employees from political coercion in the workplace, and it ensures federal employees can move upward in their career based on merit, and not on their political affiliation.

"The Hatch Act is actually in federal employees' interest," said Turner. "You don't want to have a system where there's pressure for you to sort of go along with whatever the dominant party is."

# Accession Takes More Than Skill

*By Warrant Officer One Phillip Edwards, 781st Military Intelligence Battalion (Cyber)*

On April 17, 2018, I reached a career goal that I have been chasing for 15 years: I became a Warrant Officer! And yes, I am still in shock. It is mind-blowing to think about what has transpired over my career to reach this point. I would love to share that incredible journey of what it took to obtain the technical know-how, explain the most impactful lessons that I've learned from past leaders or the types of assignments that cultivated me, but honestly, I have a far better story to share. I hope this adventure I share with you not only proves that hard work is rewarded but to never give up when things get hard.

***"Many of life's failures are people who did not realize how close they were to success when they gave up."*** **– Thomas Edison.**

This story is equal parts heartfelt gratitude and commitment between a Soldier and his Brigade, Battalion and Company command teams. I'm thankful for their commitment to me and to each of us!

This story begins on a seemingly normal day at the office. As I sat in my cubicle preparing the work of the day, I receive a message from Warrant Officer Charland: "Congratulations."

"For what?" I asked.

"You have been selected."

I was completely stunned and excited. After the last Warrant Officer selection board, I had been labeled as fully qualified, but not selected. I had a feeling it had something to do with my permanent profile. But that didn't matter anymore…I had been selected.

Astonished and nervous about this news, I headed to the HRC (Human Resources Command) website to see the results for myself. There it was, in black and white; I was selected. I still feel the excitement of that moment and am sure it is something I will never forget.

Soon after the selection list was posted, I received orders for Warrant Officer Candidate School (WOCS) and I set my sights on conquering the challenges of this school, not fully understanding the unforeseen challenges ahead.

Weeks after the congratulatory messages and emails ended, I started to wonder where my Army Physical Fitness Test (APFT) wavier was and how to obtain a copy. I knew that it would be needed for in-processing, so I grew eager to get a copy. During my search, I discovered that the waiver was missing from my request and was pending a decision from the Army G3/5/7. On May 1, 2017 I received information from the Army G3/5/7 that my request was denied. I recalled the outcome of the last board and felt utterly defeated. I'd been disapproved a second time for the same reason. It was like a good dream turned nightmare. To be told one moment, you have been selected, then in an instant, it was gone. I was mentally tallying up the you-failed-again signposts on my road of failure. My thoughts began to spiral. At the time, I was going through a nasty divorce and pending custody battle. To be honest, all of it together was extremely stressful.

Before the proverbial ink could dry on that May 2018 email, my company commander, Capt. Travis Siemion quickly came to my aid. I truly believe that he sowed the foundational support I needed to submit an appeal. It wasn't long before all of our leaders put me on their calendar. It is amazing to think how many senior leaders gave me their time to allow me to ask for their support and guidance on this matter. I believe the keys to my success ultimately came from the hard work and dedication to our Soldiers, our mission, and our unit.

I would like to share two key moments with you that remain at the forefront of my mind. When I attended the meeting with Lt Col. Justin Considine, the commander of the 781st Military Intelligence (MI) Battalion, his confidence for a positive outcome never wavered. He helped me gain a sense of balance, to be both realistic and resilient. I couldn't have asked for better guidance during this difficult time. Later, the

unit set up a meeting for me to meet with Brig. Gen. Jennifer Buckner, the deputy commander of the Cyber National Mission Force. Again, I was stunned and amazed at our cohesiveness. As I sat across from her in the command suite conference room of U.S. Cyber Command, she expressed the difficulty of this task, and then provided clear and optimistic guidance for me to follow. Before being dismissed I was reassured with a kind and commanding, "I'll do what I can Sgt. 1st Class Edwards and make a few calls."

Armed with guidance to provide more details about my injury, I quickly started working on my appeal. My first task was to find my former company commander, now Army Reserve Lt. Col. Adam Korenyi-Both and ask for his help in the form of a memo to the board explaining what had happened during our deployment. I haven't seen or spoken to the man in over 12 years, how was I going to find him and would he even remember me? I lucked out and found him on a Facebook group with all my former unit members. I sent him a message asking if he would mind giving me a call. A few hours later he called. I explained the situation. Without hesitation, he agreed to help. It wasn't long before I received his memo.

During this time, I received memorandums of support from every level within our command. My appeal packet was complete. I nervously scanned the documents and sent them to the directed point of contact at Army G3/5/7, then waited. Two days later, I was on my way home from a Bravo Company teambuilding event when I receive a call from Command Sgt. Maj., Cecil Reynolds

"Did you see the email?" he asked?

Before I could explain that I hadn't, he told me that he had the result of the appeal.

"Congratulations," he said.

I had won my appeal! I was going to Warrant Officer school, for real this time. We continued to talk briefly, but the lasting takeaway was that he was proud that I never gave up. He commended me for displaying true professional class and resiliency. I hung up knowing I would remember that conversation and how I felt for a long time to come.

Moments after ending that call, Capt. Siemion called to tell me the news. I am sure he wanted to be the first one to tell me, but it is tough to beat a Sergeant Major to good news. We shared a conversation that recalled all of what you've read and some that I simply could not capture in this story. As you would imagine, I could not wait to read the email. I quickly booted up my home computer and logged on to our enterprise email system. At the top of the email listing, there was one unread email: my results. Attached was an approved APFT wavier from Lt. Gen. Joseph Anderson, Deputy Chief of Staff, G3/5/7 signed on June 30, 2017.

I am truly humbled and thankful to every leader that supported me. I wear the rank of warrant officer proudly. I could not have done this on my own, but I do believe that our Army rewards those who embody the warrior ethos, both on the battlefield and in garrison.

To every Soldier:

Remember to always "place the mission first." You will earn what you put into our Army;

Be remembered, work hard and dedicate yourself;

"Never accept defeat," no matter the challenges, both professional and private;

"Never quit," on the mission or your dreams because you don't know how close you are to success; and

Understand that "never leave a fallen comrade" isn't just for the battlefield.

My own experience took Soldiers from our upper echelon, our Brigade and Battalion teams, and my unit commander from yesteryear to accomplish, no one left me behind.

*Courtesy Photo*

# Cyber branch direct commissions its first two officers

*By Capt. James Williams III, Cyber Center of Excellence Public Affairs*

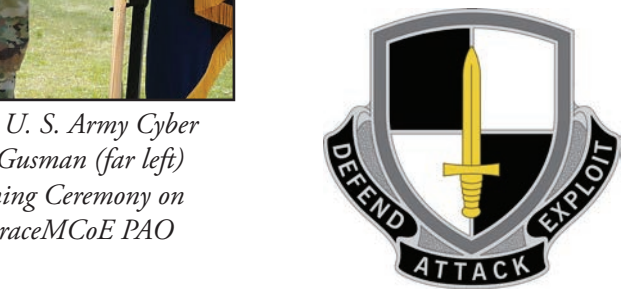
***FORT BENNING, Ga.*** *- Brig. Gen. Neil Hersey, Commandant, U. S. Army Cyber School, Fort Gordon administers the oath of office to 1st Lt. James Gusman (far left) and 1st Lt Timothy Hennessy during the Cyber Direct Commissioning Ceremony on Taylor Field at Fort Benning, May 9. (Photo Credit: Markeith HoraceMCoE PAO Photographer)*

**FORT BENNING, Ga** - 1st Lt. James Gusman and 1st Lt. Timothy Hennessy took the oath of office as the U.S. Army Cyber Branch's first direct commissioned officers during a ceremony on Taylor Field, May 9.

Brig. Gen. Neil Hersey, the Commandant of the U. S. Army Cyber School at Fort Gordon administered the oath and welcomed the new officers into the youngest branch in the U.S. Army. "I am proud of what these two officers have accomplished to be here today," said Hersey. "Though they still have more training ahead of them, they have proven to be the most competent, and to possess the greatest potential during a very competitive selection process."

To be considered for direct commissioning, applicants must hold at least a bachelor's degree and demonstrate a professional level of competence in a cyber related field. Both, Gusman and Hennessy have extensive backgrounds in multiple areas such as information technology, information assurance, cyber security or cryptology. Both have prior Army service, and were the only two among almost 80 applicants, to receive direct commissions.

The U.S. Army authorized the Cyber Branch to grant five direct commissions per year in efforts to recruit talent possessing industry experience, relevant education, and the potential to fulfill duties required by the Army.




***FORT BENNING, Ga.*** *- 1st Lt. James Gusman (right) and 1st Lt Timothy Hennessy immediately after the historical first Cyber Direct Commissioning Ceremony on Taylor Field at Fort Benning May 9. (Photo Credit: Markeith HoraceMCoE PAO Photographer)*

# COL Dave Branch
## 4th Commander
## 780th Military Intelligence Brigade (Cyber)

*U.S. Army Photos*

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)