Volume 6, Issue 3

the BYTE

780th Military Intelligence Brigade

- 780th MI Bde. Change of Command
- ARCYBER Best Warrior
- AIDP-Cyber, TDQC, and more

Sustainable Readiness

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. Brian D. Vile
Commander

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

Steven P. Stover
Public Affairs Officer
and Editor

Columns

In every issue...

Photo Pages

On the cover:
FORT GEORGE G. MEADE, Md.
– Soldiers from the 781st Military Intelligence (MI) Battalion, 780th MI Brigade (Cyber), raised our Nation's flag at reveille in a time-honored military tradition, which was even more special to be a part of on a day we celebrate our country's independence.
(US Army Photo)

Features

Articles

From the Editor

The theme for this issue is *"Sustainable Readiness."*

On May 17, 2018, Gen. Paul Nakasone, director of the National Security Agency and commander of the United States Cyber Command (USCYBERCOM) stated "As the build of the cyber mission force wraps up, we're quickly shifting gears from force generation to sustainable readiness. We must ensure we have the platforms, capabilities and authorities ready and available to generate cyberspace outcomes when needed."

Gen. Nakasone made these remarks in a Department of Defense news release after all 133 of USCYBERCOM's cyber mission force (CMF) teams achieved full operational capability.

In this issue of the BYTE we asked the command what does "Sustainable Readiness" mean to their organization from the CMF team-level up through the brigade command and staff.

"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.

PUBLIC AFFAIRS
UNITED STATES ARMY

'80MIB QRCode.pn

"Everywhere and Always...In the Fight!"

By Col. Brian Vile, commander, 780th Military Intelligence Brigade (Cyber)

Three months into command, I want to take the opportunity to thank the Brigade's Soldiers and Civilians for what you do daily to meet the challenges we face to accomplish our assigned missions. The 780th has consistently led the way in cyberspace, setting the example for the other Services to follow. However, the nature of our mission does not allow us to rest -- we are ***Everywhere and Always...In the Fight!*** To continue to be successful, every member of the Brigade must understand the vision for the Brigade:

"The 780th provides America's most innovative cyber-space operations force, deterring, and when directed, defeating our Nation's adversaries in and through cyberspace."

Maintaining the status quo is not sufficient. Cyberspace changes too rapidly to allow us to rest on past accomplishments. Unlike the conventional domains, cyberspace is in a constant state of change: new capabilities and technologies are introduced, known vulnerabilities are patched, and thousands of changes are made. Our continued success in this environment requires innovation at every level.

Innovation is simple in concept, but difficult in practice. Innovation will require every Soldier and civilian to be agile, adaptive, and opportunistic; to operate collaboratively; and to never stop learning.

Agility is the ability to move, adjust, and make decisions quickly. Adaptability is the ability to do so when faced with unfamiliar situations. By maintaining an agile and adaptive mindset, we will be postured to take full advantage of opportunities as they present themselves. Leaders must exercise mission command through mission orders, accepting prudent risk and exercising disciplined initiative to seize opportunities and counter threats within the Commander's intent. Minimize detailed instructions; allow subordinates the greatest possible freedom of action. For the mission to be successful, every Soldier and civilian must think agility and adaptability, and be empowered to seize every opportunity. This is the foundation of innovation.

We will not achieve success in our domain through individual innovation; instead, it requires a collaborative team approach. Collaboration is not just limited to occurring within our crews, sections, or teams. Instead, it must occur both laterally and horizontally; with our peers facing similar problems, and with our higher headquarters and down to the individual level. The technical scope and breadth of cyberspace is staggering; anyone who declares themselves an expert in all areas is ignorant or arrogant, or a dangerous combination of both. We must network outside of our ranks, teams, and Service in order to identify the best solutions, wherever and with whomever they reside. We must work with our supported commanders in order to fully appreciate what tasks they need accomplished, and how it fits into their Commander's intent. Collaboration will help us ensure that we don't solve the same problem twice, and that every ounce of ability within the Brigade and Cyber Mission Force is used to its maximum potential.

Finally, innovation will require every member of the Brigade to dedicate themselves to continual learning, not only within the field of cyberspace operations but to related fields that make us more effective. Cyberspace is in constant flux; new code and associated vulnerabilities are introduced daily, and every day network defenders implement new measures to mitigate the risks. This change provides vulnerabilities appear and disappear as patches are applied and software updated. By keeping our knowledge up to date and relevant, we will be prepared to seize every opportunity and achieve maximum advantage. But we must not limit our learning to technical issues; cyberspace exists to create benefits in the real-world. Understanding

Continued on page 38

"Sustainable Readiness" – the Battle of Time Management

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

Sustainable readiness is an easy concept, but a very difficult process.

For the 780th Military Intelligence Brigade, sustainable readiness has several meanings to include: completing 350-1 training; being medically ready to deploy; maintaining physical fitness; pursuing professional military education opportunities; and competing training and certification in a work role. This culminates at the team level where each team must certify as ready to accomplish their assigned mission. Each of these tasks take time to accomplish and in some ways, none of them are easy. The pressure to accomplish the mission, sometimes at the expense of overall readiness, can detract from sustainable readiness, putting the Soldier, Civilian, or even the team in a readiness hole from which they will have to crawl out. Falling behind in readiness and having to play catch-up is not sustainable and can lead to team fatigue. It is much better to maintain readiness, being proactive vice reactive, than trying to "jump through hoops" to retain a state of combat readiness.

On the Army side, we must pay attention to the expiration dates of our 350-1 training; know when our next physical fitness test is; know when our medical and dental exams are due; and what professional military education we need to advance in our military career. Do not wait until you are delinquent, take care of it before you fall out of tolerance. This way you can plan in advance on when you want to accomplish the task and do not have to take immediate action to correct a deficiency. Kenneth Blanchard, author of "The One Minute Manager Meets the Monkey", sums responsibility for readiness up best: "The way to develop responsibility is to give them responsibility." It is your responsibility to maintain personal readiness.

On the operational side, sustainable readiness can be much more difficult. The training pipelines our personnel have to navigate through to become trained and certified in their assigned work role are difficult and very time consuming -- the prerequisites don't necessarily line up; courses are not always available when needed; there are training conflicts; and sometimes life happens and we are not available for the training.

Whatever the reason, 10 to 12 weeks of training can take up to a year to complete. This can have profound impacts on the readiness of the team and the team's ability to certify as capable of accomplishing its mission. We are limited in our ability to impact much of this process. Where we can help is to be agile and adaptive, always ready to fill a seat in a class when one opens up suddenly. We must pay attention to class fills and immediately take action to fill that seat as soon as possible. We are in a competition with every other service and our partners for open seats in classes. Delay will cost us a seat that we can use to get one more person training to certify in their work role. We need to make the best use of every opportunity we have to get our personnel trained and certified in their work roles. This will lead to the long term success of our organization.

NCOs, this is your responsibility. Officers are in charge of training, but we are responsible for ensuring it is conducted. First Sergeants, Platoon Sergeants, Squad Leaders, and Team NCOICs, it is your responsibility to ensure your personnel complete the training needed for sustainable readiness. You are the key in ensuring your personnel are ready to perform their duties as members of the unit. Seek out every opportunity to give your Soldiers the edge so that they can meet both Army and operational requirements and be ready when and where the Army needs them. Our motto says it all, ***"Everywhere and Always…In the Fight!"*** We are always engaged with the enemy. Sustainable readiness is the only way we can continue to perform our mission, now and into the future.

A change in Cyber Brigade

By Steven Stover, public affairs officer,

FORT GEORGE G. MEADE, Md. – Col. Dave Branch (right), the outgoing commander of the 780th Military Intelligence Brigade (Cyber), passes the brigade colors to Maj. Gen. Gary Johnston, commander of the U.S. Army Intelligence and Security Command (INSCOM), during a change of command ceremony on the McGlaclin Parade Field June 14. (U.S. Army Photo)

FORT GEORGE G. MEADE, Md. – Col. Dave Branch relinquished his command of the 780th Military Intelligence Brigade (Cyber), after two very successful years, to Col. Brian Vile in a change of command ceremony hosted by Maj. Gen. Gary Johnston, commander of the U.S. Army Intelligence and Security Command (INSCOM), on the McGlaclin Parade Field June 14.

Maj. Gen. Johnston spent a significant portion of his time, both before and during the ceremony, praising Col. Branch and highlighting the “momentous and memorable” achievements of the brigade Soldiers and Army Civilians during his tenure as its commander.

“The 780th is affiliated with a lot of units, INSCOM, U.S. Army Cyber Command, the Cyber National Mission Force, multiple Joint Forces-Headquarters, and the entire intelligence community,” said Johnston. “The Army and the Nation recognizes what you do for the cyber force. Throughout all the efforts of the counterterrorism fight, things that you are doing in Afghanistan and Iraq, are just amazing. Your mission is vital to the intelligence enterprise, to the operators, and your activities are clear evidence of the significance of what you do.”

Johnston, whose previous assignment was in Afghanistan, said he was the beneficiary of the efforts of the 780th and couldn’t thank the organization enough.

“During the last two years the 780th has become a multi-faceted unit, using all-source intelligence, signals intelligence, open source intelligence, to inform teams and secure infrastructure, providing

leadership is a mixed blessing

780th Military Intelligence Brigade

informed intelligence support to cyberspace," said Johnston.

He then discussed the brigade's accomplishments in the previous two years under the professional and calm leadership of Col. Branch, including running nonstop operations in response to the demand.

"Under Col. Branch's command of the 780th, you supported multiple commands of four different combatant commands. You brought 21 cyber mission teams to full operational capability, the first of any service to meet this milestone achievement," said Johnston. "Whether 780th was implementing a unique cyber crew team training model or expanding cyber capabilities to Corps and below, Col. Branch's innovative approach ensured unit development, measurable standards, and successful outcomes."

"You didn't just focus on today's fight, you were focused on tomorrow's fight," said Johnston. "By supporting four National Training Center rotations, fully integrating cyberspace elements into expeditionary cyber support teams, embedding with the unit during home-station training, as well as during the rotation itself."

Maj. Gen. Johnston closed his remarks by welcoming Col. Vile and his Family to the INSCOM team and the cyber force. Vile is coming from his last position as the deputy director of the U.S. European Command's Joint Cyber Center where he synchronized and integrated cyberspace operations into the command's plans and operations. He is a former infantry officer with operations cyber and information operations experience.

FORT GEORGE G. MEADE, Md. – Col. Brian Vile (left), the commander of the 780th Military Intelligence Brigade (Cyber), accepts the brigade colors from Maj. Gen. Gary Johnston, commander of the U.S. Army Intelligence and Security Command (INSCOM), during a change of command ceremony on the McGlaclin Parade Field June 14. (U.S. Army Photo)

Continued on page 41

Cyber Legion: "Sustained Readiness"

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

Conducting combat operations in the cyberspace domain is a continuous and complex endeavor. This complexity brings unique challenges in terms of both individual and collective training for our Soldiers and Army Civilians. Achieving that level of training proficiency for one team, one time is difficult. Sustaining that training over time for all Combat Mission Teams (CMT) and Combat Support Teams (CST) is another matter.

Each of the eight CMTs and six CSTs of the Battalion are decisively engaged in supporting their combatant commander's cyberspace objectives. The intense focus of the teams can often have the feeling of a deployment, in the sense that it is both continuous and demanding. The focus comes with a cost. There are no force regeneration cycles and, to date, there are no "green, amber, red" cycles. This creates the leadership challenge to maintain and improve individual and collective skills.

The first challenge is individual training or developing skills of new team members to a point where they can contribute. Soldiers undergo at least a year of basic and advanced individual training prior to arriving to the Battalion, followed by an additional 6-24 months of training just to be assessed at the "Basic" skill level in their Cyber Mission Force (CMF) work role. Building a Senior or Master analyst, developer or operator can take upwards of five years or more.

The second challenge is performing periodic collective training, to enable the team of operate as a team. This is critically important, because our day-to-day operations do not always reinforce the notion of team.

The Cyber Legionnaire has overcome both challenges. Responsibility for individual training falls on team leaders, company command teams, company training rooms and the battalion's S3 shop. The group did a phenomenal job over the last several years ensuring our Soldiers and civilians received the required training. While not always a smooth process, the group seized opportunities. We will continue to push on individual training. I am most optimistic when I remember that the Army's Cyber Branch is relatively young, at only four-years old. As our force matures, the breadth and depth of experience that individuals possess in cyberspace operations will increase. Our Soldiers and Army Civilians will achieve the Senior and Master levels of expertise. They will become the mentors of the future, junior members of the force.

On the collective training side, the responsibility again falls to the team leads, company command teams, and the S3 shop, but both our battalion and brigade exercise planners and assessor cohort also do much of the heavy lifting. Several of teams recently completed validation exercises that demonstrate to themselves, the battalion and brigade leadership, and senior Army leaders that each team is ready to perform. Finally, the battalion's leaders have collectively recommitted to producing and implementing lessons learned over the course of the next year.

Special thanks to the S3 training team, company and detachment training NCO's and specialists and our assessor team including: Mrs. Hamilton, Mrs. Manassa, Mr. Staley, Mrs. Johnson, Mr. Bragg, SSG Folsom, SPC Vo, SGT Root, SGT Alcala, SSG Henry, SSG Omara, Mrs. Young, Mrs. Gallogly, CW4 Rudy, and Mr. Franklin.

In closing, the Battalion continues to successfully face the tough challenge of sustained readiness while simultaneously remaining decisively engaged in offensive cyberspace operations and signals intelligence. The men and women of the Cyber Legion continue innovate and lead change while remaining "Everywhere and Always…In the Fight!"

"Cyber Legion...Silent Victory!"

Army's BCT cyber teams to double in size

By David Vergun, Army News Service

FORT IRWIN, Calif. *– Soldiers from the Expeditionary Cyber Support Detachment (ECSD), 782nd Military Intelligence Battalion (Cyber), based out Fort Gordon, Georgia, pause to pose for a picture with their battalion commander, Lt. Col. Matthew Lennox, and battalion senior enlisted leader, Command Sgt. Maj. Bart Larango, at the National Training Center May 31. (U.S. Army Photo)*

WASHINGTON -- Combatant commanders are increasingly getting better support in the cyber domain thanks to a diverse group of problem solvers, said Lt. Col. Wayne A. Sanders.

Sanders, chief of the Cyber-Electromagnetic Activities Support to Corps and Below Program, U.S. Army Cyber Command, spoke Aug. 2 at the Association of the U.S. Army's Cyber Hot Topics panel.

After each of the past 10 combat training center rotations and numerous deployments, these problem-solving cyber operators have been learning something new each time and are improving and integrating better with the staff of the maneuver commanders, he said.

As a result of learning from those 10 CTC rotations and lots of assessments from the Cyber Center of Excellence and other commands, a determination was made to double the size of cyber teams supporting brigade combat teams from five personnel to 10, he said.

Each of those teams will be led by a major who has a "17B Cyber Electromagnetic Activities Officer - Electronic Warfare" military occupational specialty, and a captain, with a "17A Cyber Operations Officer" MOS, he said. Teams will include offensive and defensive cyber, as well as electronic warfare and information operations Soldiers.

The other big development is that the secretary of the Army authorized the creation of a cyber warfare support battalion, he said. Initial operational capability for that battalion will be in fiscal year 2019, which begins in October.

The battalion will go after gaps in cyber against peer threats, he said. Those personnel will find the software and hardware solutions that will make the cyber teams more innovative and expeditionary.

Sanders said that in every single operation that cyber teams are a part of, they learn something new during their forensic analysis of attacks. That information is then shared with cyber teams throughout the Army.

A lesson learned could be about a new tactic or technique used in a cyber or electronic warfare attack, he said. Or, it could be about something totally unrelated.

He provided an example. During a recent deployment, the cyber team assigned to the maneuver commander found out after hitting the ground that transportation was not readily available.

Continued on page 42

"America's pioneers in cyberspace" Vanguard

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

FORT GEORGE G. MEADE, Md. – Lt. Col. Justin Considine (right), the outgoing commander of the 781st Military Intelligence (MI) Battalion (Cyber), passes the battalion colors to Col. Brian Vile, commander of the 780th MI Brigade (Cyber), during a change of command ceremony on the McGlachlin Parade Field Aug. 1. (U.S. Army Photo)

FORT GEORGE G. MEADE, Md. – The departure of a respected leader can be a difficult event for the Soldiers and Army Civilians of any organization; however, the Army is a close-knit Family, never truly saying goodbye to those who leave and always welcoming new members into the Family.

Lt. Col. Justin Considine, the outgoing commander of the 781st Military Intelligence Battalion (Cyber), the Vanguards, relinquished his authority to Lt. Col. Nadine Nally in a change of command ceremony hosted by Col. Brian Vile, commander of the 780th MI Brigade on the McGlachlin Parade Field, Aug. 1.

In his remarks to the distinguished guests, Vanguard Soldiers and Civilians, their friends and Family, Vile stated the battalion has proven itself to be "America's pioneers in cyberspace", and the organization has earned its "well-deserved reputation for competence and excellence".

Vile then highlighted the unit's achievements in the two years Considine has commanded the 'Vanguard' battalion.

During his tenure all nine (cyber) teams achieved full operational capability and are actively engaged in cyberspace; the unit successfully integrated cyber support to tactical forces during four rotations at the National Training Center; the Cyber Solutions Development detachment is regularly producing

changes leadership

new capabilities; the expeditionary company is ready to deploy to areas of hostility on short notice to integrate cyber effects into tactical operations; the Mission Support Platoon is providing Open Source Intelligence reporting to National Mission Teams; the battalion has a new headquarters located in a world-class facility; the unit has successfully completed a pilot to demonstrate the power of unity of command; and the organization is hosting and teaching their own (cyber) mission commander course.

"Despite those accomplishments, your support to the Cyber National Mission Force was the hallmark of your command," said Vile. "You fully dedicated yourself to supporting the commanders' requirements, regardless of how challenging or difficult the task was to accomplish. You managed your Soldiers, the mission, and sustainment requirements flawlessly."

In his following comments, Considine deflected the credit for his battalion's significant achievements toward his Soldiers and Army Civilians.

"All of these accomplishments would not have been possible if it had not been for the service and sacrifice of the Soldiers and Civilians of the 781st MI Battalion and its many partners," said Considine. "The quiet professionals that give the Vanguard its identity as a team of trail-blazers that are always testing the boundaries of what can be achieved in and through the cyberspace domain. Simply put, it is the men and women of the Vanguard that I am most proud of, reminding me every day that people will always be our most decisive advantage in any domain."

FORT GEORGE G. MEADE, Md. – Lt. Col. Nadine Nally (left), the commander of the 781st Military Intelligence (MI) Battalion (Cyber), accepts the battalion colors from Col. Brian Vile, commander of the 780th MI Brigade (Cyber), during a change of command ceremony on the McGlachlin Parade Field Aug. 1. (U.S. Army Photo)

Continued on page 42

Losing the fight and not knowing it: Lessons

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

In October of 1805 the Royal Navy, under the command of Vice Admiral Horatio Nelson, delivered a crushing defeat to the Combined French and Spanish fleet. Outnumbered 27 to 33, Vice Admiral Nelson applied creative genius to win what would become the most famous naval battle of the Napoleonic wars. The battle is often used as a lesson in leadership and the effectiveness of empowering subordinates. However, the proverbial “story behind the story” teaches us valuable lessons in readiness. Unknown to the French-Spanish fleet, their readiness practices likely determined their defeat before the first shot was ever fired.

Based purely on the numbers of ships and guns, the odds of the battle seem overwhelmingly against the British. However, it is important to note the state of the French-Spanish fleet. The battle occurred near the Spanish port of Cadiz. Driven by an insatiable demand for victory, the French had long delayed critical repairs to their ships due to a lack in deep water harbors. As the fleet fell into disrepair, they found themselves constantly behind in maintenance; wearing out ships just as fast as they could repair them. Going into the battle, a non-insignificant number of the Combined fleet was barely serviceable according to military standards. When compared to the British, who preferred to keep their ships immaculate and relatively well-maintained, the Combined fleet was actually fielding fewer battle ready ships.

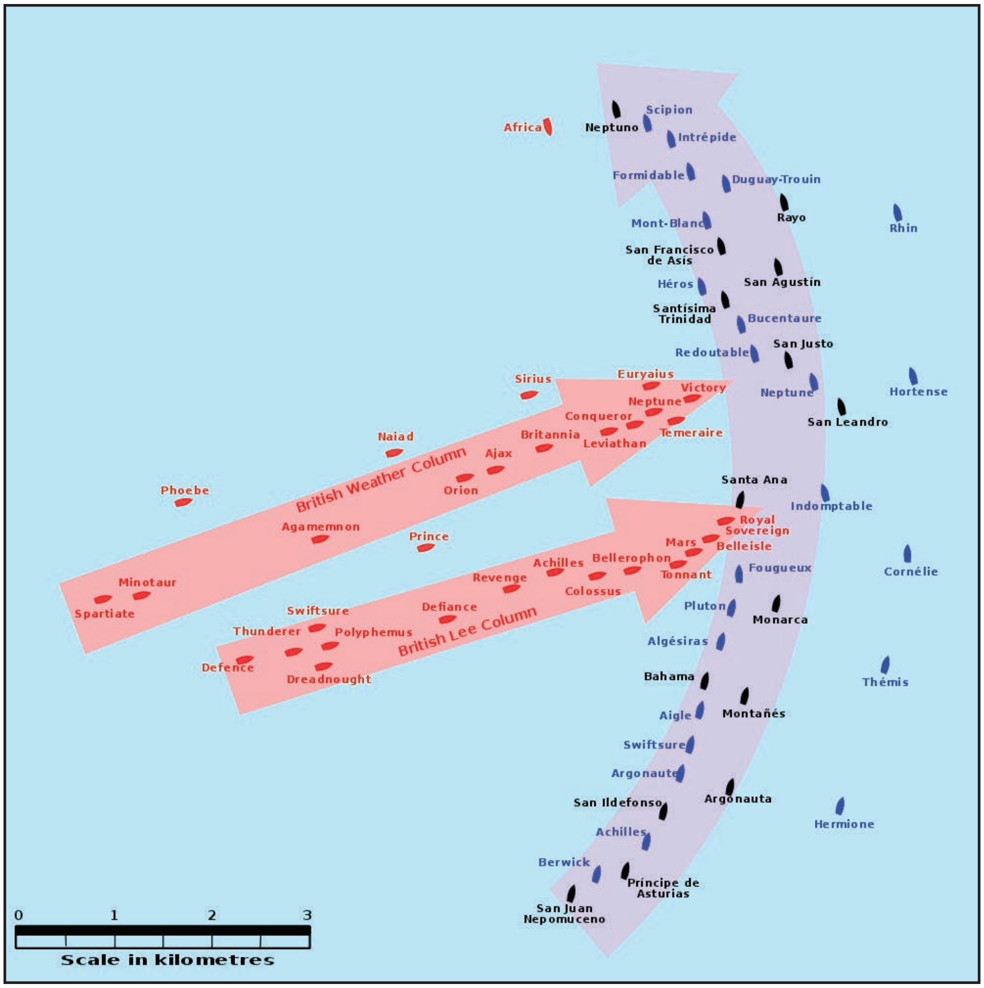
Adoption of technology and capability has always provided militaries with decisive combat power and force multiplication. In 1805, technological improvements in naval gun firing mechanisms had recently been developed. Previous firing mechanisms required fuses which delayed the time from “trigger pull” to actual firing. This made accuracy difficult in naval conditions where pitch and roll of the tide made a steady sight picture nearly impossible. The new gunstock firing mechanism technology allowed naval guns to be fired instantly upon the pull of a cord. This meant that the ship’s captain could ensure accurate and constant rates of fire. Unfortunate for the Combined fleet, they were slow to adopt this technology. The difference in firing mechanisms may not have been a noticeable hindrance beforehand. However, at the Battle of Trafalgar, where tides caused a constant pitch of up to 20 degrees, the Combined fleet undoubtedly recognized their folly. The Royal fleet had not waited to adopt this technology. Both their sailors and captains were trained and ready

Battle of Trafalgar by Clarkson Frederick Stanfield, 1793–1867 (This work is in the public domain in its country of origin and other countries and areas where the copyright term is the author’s life plus 100 years or less)

from the Battle of Trafalgar

to exploit this technological advantage.

Medical advancements were also a major contributor to readiness of the Fleet. During the Age of Sail the disease known as scurvy had been a constant struggle for every navy. The disease would cause weakness, fatigue, issues with limbs, etc. Some historians describe the French-Spanish fleet at Trafalgar as “floating hospitals” due to widespread illness. The most unfortunate part is that European doctors had discovered a solution to this problem years prior to Trafalgar. It was determined that regular consumption of citrus would prevent and cure scurvy. The Royal Navy quickly ensured that every ship was well stocked with limes before departing for sea (earning their sailors the nickname of ‘limey’). Hence, at the Battle of Trafalgar the sailors of the Royal Navy were in far better health than their French-Spanish adversaries.



This map of the Battle of Trafalgar shows the approximate position of the two fleets at 1200 hours during the battle as the Royal Sovereign was breaking into the Franco-Spanish line. North is to the top, and Cape Trafalgar is 10 miles to the northeast (Permission is granted to copy, distribute and/or modify this document under the terms of the GNU Free Documentation License).

The last readiness correlation to draw is in regards to training. The way the French-Spanish fleet trained and validated their force was woefully ignorant and insufficient. Selection of French naval officers was a combination of lineage (or social status) and mathematical examination. They were then trained according to mostly land-based military techniques and philosophies. This led to French officers employing naval ships as floating fortresses from which to conduct land-style battle. In fact, most French naval captains lacked interest in sailing entirely and would delegate such tasks to junior officers without giving them any meaningful guidance. The Royal Navy could not have been more different. Royal Navy officers were selected from amongst the professional and worker classes just as much as the aristocracy. Prior to being commissioned these aspiring officers would require six years at sea as midshipmen; being mentored by experienced captains and sailors alike.

Before being commissioned they would be tested on their leadership as well as their expertise as a sailor. When it then came to battle, the captains and their crews trusted each other and were trained in employing their vessel effectively in the sea domain.

Continued on page 43

01 National Mission Team re-certification

By 1st Lt. Lance Jones, executive officer, Bravo Company, 781st Military Intelligence Battalion (Cyber)

In order to maintain optimal operational readiness, 01 National Mission Team (NMT) conducted a Live Fire recertification Exercise (LFX). 01NMT utilized a hybrid model that combined real world operations with conducting a realistic training exercise. The underlying premise of the model was to demonstrate the ability to train our Cyber Soldiers to the highest standard while maintaining a high operational tempo. During the lead up to the recertification, 01 NMT's mission development was expanding and evolving from a team centric, hostile-actor focused mission, to a Task Force driven, key terrain focused, operational approach. The effort was not simply to thwart the adversary but to identify and develop multiple options based on various threat courses of action. The recertification exercise was a success! Key leaders noted the short falls identified during the evaluation and will implement mitigations into future training plans.

01 NMT dedicated six months to training the Soldiers, while detailing and preparing the scenario. The officers and non-commissioned officers (NCOs) in-charge focused on executing three phases leading to the LFX— 1) the individual battle drills; 2) crew drills; and 3) the In-stride assessment. Leaders meticulously planned and executed all phases while managing the Cyber National Mission Force's high operational tempo. The operational tempo was the driving force behind executing an in-stride assessment for the non-cyber supporting crews, and using a live-fire-exercise to assess the firing crew's ability to deliver cyber effects in support of the mission commander.

The in-stride assessment started as a team of elite Brigade assessors conducted a review of day-to-day operations. Over a five day period, the assessor team evaluated the teams analytical briefings, tactics, techniques and procedures. Each analyst delivered in a major way as they executed critical team skills as developing effective mission profiles, preparing and delivering line-of-effort briefings, and occupying cyber fighting positions.

Following the in-stride assessment, 01 NMT broke the team into five firing crews, to conduct the live-fire portion of the evaluation. The five-day LFX focused on the team's ability to conduct information collection, execute the joint targeting process, and deliver cyber effects against a fictitious enemy in the cyberspace domain.

01 NMT's warrant officers and NCOs collaborated their expertise to develop the LFX virtual network range and configured it to reflect its real world target set. The execution of the LFX was interlaced with standardized cyber-control processes and emphasized the inter-relation of operations and intelligence activities.

More than a standard capture-the-flag exercise, the team-created environment emphasized the development of maneuver pathways through the target network. The platform identified and characterized target elements during surveillance and reconnaissance missions in support of follow-on offensive cyber operations.

So what's next? The 01 NMT is wrapping up the engagement by documenting LFX development and execution efforts, and recording after-action review comments to facilitate interested teams' use of the virtual environment for their own collective training needs. 01NMT has shown that they are a pioneer for conducting concurrent training while maintaining a high operational tempo. Their success during the LFX, displays 01NMT's willingness to adapt, eagerness to improve and efficiency to execute.

Sustainable Readiness

By Capt. Mark Klink, commander, Charlie Company, 781st Military Intelligence Battalion (Cyber)

In the spirit of this month’s theme, maintaining both operational and administrative readiness for the Cyber National Mission Force (CNMF) is quickly becoming a topic of hot discussion. While we’ve refined how we track the readiness of maneuver forces over the course of decades (and arguably have yet to find a perfect solution), we lack the breadth and experience to understand what a ready and available cyber mission force looks like. In this short article, I’ll outline the problems as I currently see them from my foxhole and provide a recommendation towards a different process for certifying Cyber forces, but I will not, and cannot attempt to solve the issue of Cyber

There exists a tendency in the Army, or any organization, to focus on things that are tracked, reviewed, and discussed at higher levels of leadership. If we can’t measure the success of a particular task, we will never be able to improve, but if we don’t evaluate a task, we will never know how we measure. Unfortunately, under the current operating construct, our operational command and service components track elements differently (Task Forces and teams respectfully). This disconnect is further exasperated when evaluating readiness, training, or even operational employment.

Clearly, there is a concern if we are measuring the success of a larger joint task force against the certification of 30-40 Army personnel, many of whom perform different functions for the task force (TF) than they do for their team. The following is a proposal, based on extensive input from individuals at the tactical edge, for moving towards a Task Force certification process in an attempt to solve the question of how we measure the readiness of our Cyberspace elements within the CNMF.

The current team-based certification process fits the needs and the force structure for teams supporting the Service, Department of Defense Information Network, and Geographic Commands. But the CNMF was given the specific directive of task organizing their workforce in such a manner that would optimize their effectiveness to better counter their assigned adversary. While each Task Force organized differently, in order to fit their size, adversary, and experience levels, the new TF’s are better equipped for training, readiness, capability, and capacity when assessed as a combined/joint force rather than under the former team construct. From the perspective of an operational commander, the Task Forces provide increased depth in work roles, cross functional analysis capabilities, and the ability to share training and experiences across the different armed services. From the service component’s perspective, the benefit lies in the depth of work roles, allowing for minimal impact to the operational mission when fulling routine administrative requirements.

The predominant issue is the current model for exercises and assessments fails to test the full spectrum cyber space operations capability of the operational cyber element, the Task Force. Instead, we conduct our exercises in disconnected environments that prevent the possibility of any real collaborative efforts between the offensive and defensive cyber teams. The separation of networks also limits how tipping and cueing functions between the offensive cyberspace and defensive cyberspace operational elements. While the previous two points may appear to be separate issues, this all recapitulates the inability to train as we fight. The bottom line is we currently assess our CNMF forces in a manner which is counter to how we employ those same forces.

In order to solve the issue of full spectrum Task Force certifications, the training and readiness manual published by U.S. Cyber Command which dictates the responsibility to the Joint Force - Headquarters and CNMF to conduct exercises and assessments of their respective teams, needs to be amended to specifically allow CNMF to conduct and assess these events as Task Forces.

Continued on page 43

CPT Sustainable Readiness

By Capt. Sonja Brown, commander, Delta Company, 781st Military Intelligence Battalion (Cyber)

The Army’s global, operational environment remains complex and chaotic. Even as the military shrinks and global threats rise, we face a wide variety of challenges from cyber adversaries to natural disasters. Two years ago, the Army moved to a new unit “sustainable readiness” model which is about being ready to conduct the full range of military operations at any given moment. Three descriptive modules are included in this design:

- Mission Module: units allocated to or assigned to an ordered mission. These units are validated, fully resourced, and immediately ready to conduct Decisive Action operations if required. The Army describes Decisive Action as “the continuous, simultaneous combinations of offensive, defensive, and stability or defense support of civil authorities’ tasks.”
- Ready Module: units are achieving or sustaining a baseline level of Decisive Action proficiency and the ability to respond to contingencies. These units can be deployed on missions if required.
- Prepare Module: units are rebuilding readiness and not involved in missions.

In the cyber domain, Cyber Protection Teams are not unversed in these terms and the sustainable readiness model is in full effect.

In order to accommodate the two-thirds combat readiness for cyber contingencies by 2023, the 780th Military Intelligence Brigade and Cyber Protection Brigade has pushed forth the Mission Element Model to Protection Teams in order to provide defensive crews on a moment’s notice. The benefit of this structure allows teams to deploy compact crews with key network and system operability skills, which can defend and lure out adversary activities on Department of Defense networks.

Each team will be comprised of two Mission Elements (ME), comprised of two compact crews, and a Support Element. As the Army was the first of the services to reach 100% Fully Operationally Capable teams, the “mission module” was already in effect: Army cyber teams were ready to conduct decisive actions operations if required. Because the Permanent Change of Station (PCS) cycle is stranger to no service, and as Soldiers become unavailable, one crew – or even members of the Support Element - could be designated as the training crew and allow the Team to sustain greater than two-thirds combat readiness. The team would thus be downgraded to the “ready module,” sustaining or achieving a baseline level of decisive action proficiency and the ability to respond to contingencies if necessary. If the PCS cycle coincides with Soldiers’ retirements, expiration of term of service (ETS), and potentially use or lose leave, teams would be allotted the downgrade to the “prepare module,” where rebuilding and retraining would be paramount and other teams would move to the forefront to answer the call.

The introduction of the Mission Element Model provides Cyber Protection Teams with greater flexibility than the Army Force Generation Model as it addresses stabilizing manning to avoid sudden readiness declines, and prioritizes unit readiness. Additionally, with the support of Human Resource Command (HRC), teams are able to sustain higher levels of readiness over longer intervals. This provides leadership with greater readiness visibility and permits forecasting of readiness out to the next three to four years.

During the last 15 years it was the Army’s policy to ‘equip, train, and man.’ With the sustainable readiness model, the Army has moved to a model which mans the unit and then equips it, as manpower - team power - wins wars. The challenge only comes when Cyber Protection Teams deploy and redeploy, and the resulting changes in technology impacts the equipment they will need.

New facility opens to house nation’s Cyber Mission Force

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

Col. Dave Branch, the former commander of the 780th Military Intelligence (MI) Brigade, was the keynote speaker in a ribbon cutting ceremony on May 30th at a new U.S. Army Intelligence and Security Command (INSCOM) facility in the Fort Meade area which is now officially the home for several INSCOM units.

The facility will house the 781st MI Battalion and the Cyber Solutions Development detachment, both subordinate units under the 780th MI Brigade; the 310th MI Battalion, 902nd MI Group; and could house other INSCOM elements in the future.

According to Lt. Col. Justin Considine, the commander of the 781st MI Battalion, the facility is a modern administrative office building which provides fully-equipped work spaces for personnel from the 780th MI Brigade and the 902nd MI Group, both major subordinate commands under INSCOM.

After a brief welcome to those in attendance, Col. Branch talked about the importance of the new facility and what it will mean to the Army and the Joint Force.

“What you are standing in has clearly been a dream for a while,” said Branch. “You have optimized mission command, space for consolidated capability development, and a shared operational environment for leveraging natural linkages between the 780th MI Brigade and 902nd MI Group. I think that’s the biggest opportunity as we occupy the facility and work together.”

The facility brings together the 781st MI Battalion, which conducts signals intelligence and cyberspace operations, with the 310th MI Battalion which conducts technical counterintelligence operations and support, counterespionage investigations and analysis and production.

Branch said the new facility provides a mission space tailored to enhance collaboration and partnership between the two units, and along with the developers and the hardware/software lab of the 780th, these assets would “empower (the brigade’s) mission, teams, the Army and the Joint Force.”

“We’re early on into this, but we’re operational in a lot of ways,” said Branch. “And the 902nd is quickly coming into their own (as they move into their new space) and then we’ll start to see this thing exponentially ramp up.”

***FORT MEADE, Md.** -- (From left to right) Taneshina Wright; Clyde Harthcock, deputy to the commanding general, U.S. Army Intelligence and Security Command (INSCOM); Col. Jon Clausen, commander of the 902 MI Group; Col. Dave Branch, commander of the 780th MI Brigade; Chief Warrant Officer 5 Kevin, Boughton, the command chief warrant officer for INSCOM; and Lt. Col. Justin Considine, the commander of the 781st MI Battalion, cut a Category Five cable, commonly referred to as CAT 5 cable used for computer networks, to officially open a new U.S. Army Intelligence and Security Command (INSCOM) facility in the Fort Meade area which will house several INSCOM units on May 30. (U.S. Army Photo)*

Cyber Readiness

By Sgt. 1st Class Rachel A. Watkins, Target Digital Network Analyst, A Co., 782nd MI Battalion (Cyber)

The Cyber Mission Force (CMF) is charged with planning, coordinating, integrating, synchronizing, and conducting three vital and vast activities: effective defense of the Nation, support to Combatant Command (CCMD) military operations; and security and defense of the Department of Defense Information System (DODIN). To effectively accomplish these tasks, the CMF's primary goal must be readiness. But readiness in cyberspace means something much more nuanced than anything the military has traditionally been saddled with. To be truly prepared, the Army must be able to train, not only the cyber operators but also the intelligence analysts to gain and sustain familiarity with the changing digital terrain which we find ourselves in.

The cyber battlespace is unique and daunting in that it is not constrained by such simply defined terms as a "geographical area". The enemy is not limited by military budgets, or manpower, or the rule of law that United States Soldiers and DOD Civilians hold ourselves to. Countless threat actors yield weapons of destruction against our Critical Key Infrastructure or even our democratic processes and are only limited by their ingenuity and their time. Even a malicious entity with little to no cyber acumen has a world of endless websites offering easy-to-procure, prewritten and unfathomably-adaptable code.

It is due to the truly asymmetrical and constantly evolving nature of cyberspace, that the CMF's readiness and preparedness to defend the nation and DODIN and support the warfighter through offensive cyber operations (OCO) is imperative.

Rapid adaptability to changing and evolving global telecommunications standards is crucial to the U.S. military cyber doctrine. For example, Internet Protocol version 6 (IPv6—once mostly a notional but a vital replacement for the quickly-depleted IPv4 logical addressing system) was standardized as of July 2017 and is now being used extensively, particularly with mobile devices. Additionally, the recent approval of Transport Layer Security (TLS) 1.3 TLS, and its ability to thwart man-in-the-middle (MITM) attacks, will potentially further complicate both friendly and adversarial entities' offensive posture while strengthening their defenses.

U.S. Training & Doctrine Command's lengthy timeline for plan-of-instruction (POI) revision—two to three years after the Critical Task Site Selection Board (CTSSB) determines which critical skills are needed—are cumbersome in any branch's schoolhouse, but in Cyber, they have the potential to cause an entire generation of newly-minted 17-series graduates—many of which have spent a or more year in training—to arrive at their duty stations lacking skills and knowledge crucial to their work roles. To ensure trainees are receiving the most timely and relevant training, it is critical that the revision process is streamlined, and that students have access to the latest industry-standard tools and training. The Cyber Center of Excellence at Fort Gordon, Georgia, integrates five SANS Global Information Assurance Certification (GIAC) courses into their 25D Cyber Network Defender Advanced Individual Training (AIT) and three into their Senior Leader Course (SLC). This deliberate and proactive embracement of commercial civilian training standards is crucial in defending a network against enemies who are not constrained by proverbial red tape.

Signals Intelligence (SIGINT) was the first sector of the military to delve into cyber operations, and SIGINT soldiers who trained as digital network analysts earned the N6 ASI (additional skill identifier), and were eventually converted into 35Q Cryptologic Cyberspace Intelligence Collector/Analyst military occupational specialty (MOS) the original Military Intelligence (MI) MOS formed of Joint Cyber Analysis Course (JCAC) graduates. The U.S. Army announced its intent to remove the 35Q MOS; the current 35Qs will be given the choice to request to convert to 17C, Cyber Operations Specialist, (which is an operational MOS, not an intelligence MOS) or be automatically converted into 35N, Signals Intelligence Specialists, which currently receive less than two weeks of digital

Continued on page 43

Seizing the Moment: Sustainable Readiness in the Cyber Force

By Sgt. Sean Cox, Cyber Operations Sergeant, Echo Company, 782nd Military Intelligence Battalion (Cyber)

My alma mater's football team had a motto: "Anyone. Anywhere. Anytime." I would joke about our quarterback brushing his teeth when suddenly Reggie White kicks in his door, driving him to the floor saying, "You said anyone, anywhere, any time."

It's good for a laugh, sure, but it's also how the United States Army operates. On deployment, enemy attacks and tactical opportunities appear suddenly, and Soldiers need to be ready to gear up and fight at a moment's notice. If a conflict breaks out tomorrow, we as a nation need to be ready and able to mobilize quickly and effectively, especially in those critical first few days and weeks of a conflict. Races are not won only by running faster, harder, or longer. Watch the Olympics, and you will see that the difference between a gold medal and no medal is often a fraction of a second. It is equally important to be ready to move the instant the signal comes.

While the 780th Military Intelligence (MI) Brigade is not likely to deploy en masse in the next few weeks, we still maintain our own MI/Cyber form of sustainable readiness to ensure that when the need arises, either through threat or opportunity, we are ready to do our part. In this hyper-connected digital world, online threats literally move at the speed of light. We need to be able to respond quickly to network-savvy aggressors or seize fleeting opportunities before they vanish into the ether.

In 2015, Google's ownership of google.com lapsed, and for one minute, for the low price of $12, Sanmay Ved, a random tech employee, owned that famous URL. Thankfully, Ved was not a cyber-criminal and Google got it back quickly, or else who knows what damage could have been done? On average, Google processes over 40,000 searches every second. Imagine how many devices could have been infected had a malicious user bought the domain instead. Threats can appear as quick as lightning. For those working defensive missions, we have to be ready to respond at a moment's notice.

Offensively, think back to 2016 when someone in North Korea misconfigured the nation's name server. For a few minutes, North Korea's private internet was open to the world. Matthew Bryant was able to access a number of the hermit country's websites and upload them to Github, allowing computer experts around the globe to gain their first insights into how the nation's government maintains and controls their internet. It was a rare opportunity that came as quickly as it went, but because Bryant saw something and was able to respond quickly, our knowledge of North Korea's online world is clearer than ever before.

As the United States Army's cyber force, we have to be just as ready to respond before it is too late. Does this mean we sleep in our uniforms or bunk up on cots in our offices every day of the year? No, not usually. The burnout would be insane. That's not sustainable, and the goal of the Army is sustainable readiness.

So how do we sustain our cyber readiness?

We do our jobs. We have our routines, based on experience and the advice of others. These routines allow us to move smoothly and skillfully through our regular tasks, reinforcing those critical mission skills until they become muscle memory. We engage in exercises to make sure we are not only ready to perform our job roles, but also to perform as a team. They allow us to use those skills that may not come up in our daily work often but are still critical to maintain.

Thinking about possibilities before they happen is another good way to sustain readiness. Have you ever wondered about something that you figured would never happen, so you did not ask about it? Next time, speak up. Ask that hypothetical question. "Hey, SGT Smith. If we needed to, how would we do this?" Not only does it help broaden your understanding of a topic, who knows? One day that situation may arise, and then won't you be glad you had already considered what to do beforehand?

Continued on page 44

What is the Adopt-A-School program and how does it support Fo

By Lt. Brittany Larmore, section leader, D Company, 782nd Military Intelligence Battalion (Cyber)

Shortly after my arrival to the 782nd Military Intelligence (MI) Battalion (Cyber) at Fort Gordon, Georgia, I was given the opportunity to take over the Adopt-A-School program for the Battalion. Having very little knowledge of the program previously, I didn't completely understand the true purpose of the program; however, over the last year it became very clear to me that the Adopt-A-School program is more than just volunteering at Grovetown High School. It is truly about making a difference in the lives of the students as well as giving back to the community.

> It is truly about making a difference in the lives of the students as well as giving back to the community.

To put this into context, in the Fort Gordon area there are nearly 6,000 children of military and civilian government employees who attend schools in either Richmond or Columbia County. As you can imagine, this has a large impact on the military and the surrounding communities. This created a high demand from the schools for service members to visit their school to mentor, volunteer, read to students, participate in senior capstone projects, judge school projects, and get involved in other school-related opportunities. However, with no formal way for schools to reach out and ask for the help they so desperately needed, we fell short on meeting the needs of our community. While many units built informal partnerships with the local schools and volunteered where they could, the demand was too high and again still fell short of what our community and schools required.

School Support Services worked tirelessly to fill that gap; to find a better way for Fort Gordon and its service members to give back to the community via schools in Columbia and Richmond Counties. After all that hard work, in May 2017, the Adopt-A-School program was founded.

"We wanted to do a more formal program to make [the service members' time] more equitable and touching as many students and as many schools as possible," said Melissa Barrickman, Fort Gordon school liaison official. This program partners each unit with one of the thirteen high schools across Richmond and Columbia County and their feeder schools.

The program's activities are conducted to increase public awareness of the Army's mission and to foster good relations with local communities. The mission of the Adopt-A-School program is to routinely contribute military resources and services to schools in order to nurture the intellectual, emotional, social, and physical growth of children in and around Fort Gordon. Through interaction with positive role models, the program aims to ensure that children succeed and live their dreams.

During the foundation of the Adopt-A-School program, each school principal met with their Fort

rt Gordon and the almost 80 schools it is designed to support?

Gordon counterpart to sign a memorandum of understanding. It was a statement and a promise between the unit and the school to work together and help build the community. Over the 2017-2018 school year each unit fostered connections with the high schools and contributed to its local school throughout the year.

What does that mean for the 782nd MI BN?

The 782nd MI Battalion is partnered with Grovetown High School, two middle schools, and three elementary schools. After the program kicked off last year, 782nd began supporting Grovetown High School with the main focus on the JROTC (Junior Reserve Officer Training Corps) program. The 782nd provided over 200 hours for the school year and supported several JROTC events to include their Drill and Ceremony Competition and annual fitness test. Also, 1st Sgt. Quincey Welch, of Alpha Company, volunteered to sit on the JROTC’s promotion board where their cadets are tested on Army knowledge; much like our own junior Soldiers. While I will say that we had a large impact on Grovetown High School and its JROTC program; I will add that we look forward to doing more over the next year. Working with the Adopt-A-School program and Grovetown High School we will be looking to expand our volunteering by providing mentoring and tutoring across the high school and working towards having a larger impact on the middle and elementary schools that we also support.

In March 2018 we were asked by Grovetown High School to come help grade the students in their five event Presidential Physical Fitness Test for JROTC. This test took place over the course of three days and Soldiers from the ranks of Private First Class to First Lieutenant graded the cadets. Overall, the event was an amazing opportunity for the cadets and our Soldiers. For the junior Soldiers, who had never graded a physical fitness test, it allowed them to see what their Non-Commissioned Officers do every time there is a PT test and allowed them to be leaders in the eyes of the cadets; providing mentorship and encouragement throughout the process. Seeing our Soldiers and the cadets cheer and motivate their classmates to reach their full potential is what the program is all about. Between classes we stood in the hallway with the students going to and from class. There were some that would come up and thank us for our service, others just respectfully acknowledged our presence. Just being there in the hallway, standing tall in our uniforms, had an impact.

On the last day we had time for the cadets to ask us questions about being in the military; some were as simple as taking the PT test and how hard Basic Training is, to more thought-out questions of should I be an officer or go enlisted because I want to be a linguist. It truly is a humbling experience to know that mentoring these young students can have a lasting impact on what they choose to do with their lives.

On Aug. 3, 2018, I was provided the opportunity to attend the Adopt-A-School celebration; which was meant to recognize each military unit who has contributed to local schools throughout the school year. 782nd MI Battalion received an award for providing a large number of volunteer hours while partnering with Grovetown High School. At the end of the celebration Lt. Col. Matthew Lennox and

Continued on page 44

Army Cyber's top Soldiers, NCOs excel in Best

By Steven Stover, 780th MI Bde. (Cyber), and Bill Roche, U.S. Army Cyber Command

ALEXANDRIA, Va. *– Sgt. 1st Class Deon Myers, from East St. Louis, Illinois, is assigned to the 302nd Signal Battalion, U.S. Army Network Enterprise Technology Command, and appears before a Sergeant Majors' Soldier board on day three of the U.S. Army Cyber Command Best Warrior Competition at the Humphries Engineer Center Aug. 14. (U.S. Army Photo)*

FORT BELVOIR, Va. – After more than four days and nights of grueling competition, two Army Cyber Command (ARCYBER) warriors from the Army Network Enterprise Technology Command's 21st Signal Brigade have earned the title as ARCYBER's best for 2018.

East St. Louis, Illinois native Sgt. 1st Class Deon Myers of the 302nd Signal Battalion was named Best Warrior NCO of the Year, and Groton, Vermont's Spc. Tyler Gadapee of the 114th Signal Battalion was named Best Warrior NCO of the Year in a ceremony here, Aug. 16.

The pair will go on to represent ARCYBER at the U.S. Army Best Warrior Competition at Fort A.P. Hill, Va., and the Pentagon, Sept. 30 to Oct. 5, 2018.

There the cyber warriors will compete against Soldiers from across the Army who, like them, had to win multiple unit and command competitions against colleagues who are among the Army's finest.

Each of those competitions is engineered to be physically and mentally challenging. Most – and ARCYBER's is no exception – comprise a minimum of several rigorous tasks, including an appearance before a board of sergeants major; an Army Physical Fitness Test; a series of Army Warrior Tasks and Battle Drills; an obstacle course; a written essay; a 12-mile road march; day and night land navigation courses; qualification with an array of weapons; a stress shoot challenge; and a "mystery event."

"Make no mistake about it; this isn't just about impressing a board with a few memorized answers," said ARCYBER Command Sgt. Major Sheryl D. Lyon of the competition here. "This is a tough week of challenges designed to measure the whole warrior – tactical Soldier skills, intellect, physical readiness and stamina, Army values, demeanor and attention to detail. And I have no doubt these Soldiers are up to the challenge."

In addition to Myers and Gadapee, those Soldiers included Pfc. Cameron Burgess from Monticello, Indiana, assigned to the 911th Technical Rescue Engineering Company, U.S. Army Military District of Washington; Spc. Alexander Musarra from Miami, Florida, assigned to the 782nd Military Intelligence Battalion (Cyber), 780th Military Intelligence Brigade (Cyber), U.S. Army Intelligence & Security Command; Staff Sgt. Kenwyn Peters from Tinton Falls, New Jersey, assigned to the 289th Military Police Company, Military District of Washington; and Staff Sgt. Melanie Wahl from New Smyrna Beach, Florida, assigned to the 741st Military Intelligence Battalion, 704th Military Intelligence Brigade, U.S. Army Intelligence & Security Command.

So why would any Soldier volunteer to take on the grueling Best Warrior challenge – repeatedly? Interestingly, the three Soldiers and three NCOs who competed in the ARCYBER event – diverse in so many other ways – expressed very similar reasons.

The Soldiers said competing is a "good way to set myself apart from my peers"; "to prove to everybody what I am capable of" and "to distinguish myself in my unit", while the NCOs said they are motivated by the Soldiers who serve with them.

"I wanted to show my Soldiers 'what right looks like', and even at sergeant first class we're still out here getting it," said Myers.

"My future goals are to take what I learn from these competitions and go back to my guys that are with me, train them up, and get them out here to be in the same position I am in right now," said Myers. "They are our future, they have to know it."

Myers thanked his wife and daughter, as well as his battalion and brigade, for their support in the competition. As he moves ahead to the Army-level event, he said he'll focus on pistol marksmanship and medical-related warrior tasks.

For Gadapee, who thanked his family and said he hopes to be selected for Army Special Forces and earn a Green Beret, the next step is working on his board presence, physical fitness and other related training for the Army competition.

"This is a huge reward and it's really nice to see my hard work is paying off," Gadapee said. "I am looking forward to moving on and I challenge others to compete next year."

In a departure from traditional remarks, ARCYBER commander Lt. Gen. Stephen G. Fogarty stepped into the audience at the ceremony here and talked with the competitors, praising their efforts and asking questions about the competition and how they will apply what they learned here in the future. He also said that while they came to the event from different units, with different backgrounds and jobs, they share a similar goal: to better themselves and their organizations.

"This competition challenges you physically and mentally, and that's what's needed to survive under the toughest condition of all – combat," Fogarty said. "We have to have leaders who can out-think the enemy while taking care of their Soldiers."

"So we're not only here to recognize you for what you've done over the past four days, but to make sure you take something back to your units," he added. "You'll be better leaders for what you've experienced here."

The ceremony also featured remarks from U.S. Cyber Command senior enlisted leader Master Gunnery Sgt. Scott H. Stalker, who said there's no greater title than "best warrior."

"You can do the minimum ... but you've said, 'I want to be part of the Best Warrior Competition. I want to give it everything I have, and be the best person I can be.' And I commend you for that," he told the six competitors.

But he said the real point of the competition is to groom young leaders for the greatest task facing servicemembers – being prepared and preparing their units and colleagues.

"That's what this is all about; making sure that that man or woman to the left and right have the best teammates, the best training, and they're ready," Stalker said.

All the leaders who spoke at the ceremony said that while only two participants are ultimately named "best", every one of this year's competitors is a winner who leads by example.

"I'm truly honored to serve with the Soldiers competing here this week, and I know that there are many more like them among our ranks," said Lyon. "They are the future of the Army, and that future is in very good hands."

FORT BELVOIR, Va. – *Spc. Tyler Gadapee, 21st Signal Brigade (left) and Pfc. Cameron Burgess, 911th Technical Rescue Engineering Company, run to the finish of the 12-mile road march event on the final day of the 2018 U.S. Army Cyber Command Best Warrior Competition, Aug. 16. (U.S. Army Photo)*

U.S.ARMY
MATELSKI
780th Military Intelligence Brigade
LOYALTY □ DUTY □ RESPECT □ SELFLESS SERVICE □ HONOR □ INTEGRITY □ PERSONAL COURAGE
NCO of the Year
SGT Savannah Matelski
D Company
781st MI BN

780th Military Intelligence Brigade

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

Soldier of the Year

SPC Alexander Musarra
B Company
782nd MI BN

A Soldiers bond with their community

By Maj. Steven Perry, Jr., executive officer, Task Force Echo, and CPT 173 Team Chief

While the Reserve and Guard make up approximately 38 percent of U.S. uniformed manpower, the percentage related to the American population is less than approximately two percent. The 38 percent of the Guard and Reserve have a unique representation that few can have the honor of making true; the "Citizen Soldier." The Citizen Soldier is a member of the Guard or Reserve who answer the call to duty when the Country calls upon them. They leave their families and friends, employment, and other responsibilities at home to be sent off to support the Nation's Missions. The Service Members have continuously answered the call, sometimes multiple times by supporting multiple deployments both CONUS and OCONUS.

The Army Values that are instilled in a Soldier since the beginning of their military career are observed in their civilian career and everyday way of life. This holds true with the military training as well. Soldiers continue to use their military training and values in the same career field in the civilian sector. Cyber professionals, law enforcement, mechanics, and medical professionals are just some of the sought professions by the civilian sector. The training and experience Soldiers receive from the U.S. Armed Forces significantly improves their civilian occupation capabilities. Soldiers are strongly sought out by the civilian work force. For example, the real-world experience that a Doctor in combat zone brings to the civilian occupation is something that cannot be match by a traditional Doctor who only attended medical school. This is just one of many examples of how the military provides a service both in and out of the military that has a significant impact in their community.

FORT GEORGE G. MEADE, Md. *– Army National Guard and Reserve Soldiers from Task Force Echo, who were activated to support the U.S. Cyber Command mission under the operational control of the 780th Military Intelligence Brigade, meet with their counterparts routinely to discuss training and operations. (U.S. Army Photo)*

The Soldiers' community views have changed significantly over the history of the Armed Forces. Citizen Soldiers both have and receive respect from their community and their employers which they are proud to serve and represent. This has resulted in many Soldiers becoming known as a "Soldier for Life." Soldiers have spent their entire career in the Guard or Reserve; while some Soldiers from the Active Component continue their military career when they transition into the Guard or Reserve. These Soldiers bring their unique experience into the local community that only a Service Member can offer. No other profession can match the bond that a Soldier has with the American public by defending the Army values and the nation's interest to support their communities' freedoms and way of life. Many of those members of the community will have a

and community

personal relationship with the Soldiers.

The National Guard Soldier has a dual responsibility in which only they can answer. These Soldiers are responsible for meeting both the State Mission and the Federal Mission. The Soldiers' stories are unique within itself. Traditionally, they go about their daily lives working a civilian job and at times put on a military uniform, leave their families and conduct their voluntary or mobilized obligation to their community and country. The biggest supporter, and at times the most affected by the obligation, are their families and even their employers. Soldiers' families are expected, even at a moment's notice to leave their loved ones, their civilian occupation, and lives. The family support system that each Soldier prepares them for is a constant inherited duty. The obligation to their families and their community to support the Guard or Reserve Soldier is something that helps enforce that support system. Without this, the Citizen Soldier could not continue their career in being a Soldier for Life.

Warrant Officer Corps 100th Anniversary

FORT GEORGE G. MEADE, Md. *– Celebrating the 100th anniversary of the Warrant Officer Corps, the warrant officers from the 780th Military Intelligence Brigade (Cyber), raised our Nation's flag in front of the garrison headquarters at reveille in a time-honored military tradition July 9. (U.S. Army Photos)*

Army cyber program accepts only the best MI

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

FORT GEORGE G. MEADE, Md. *– Maj. Brooks Jarnagin (right) receives a plaque from Lt. Col. Jesse Sandefer, the deputy commanding officer for the 780th Military Intelligence Brigade (Cyber), after graduating from the Army Intelligence Development Program – Cyber (AIDP-Cyber) in a ceremony at the National Cryptologic Museum here on June 1. (U.S. Army Photo)*

FORT GEORGE G. MEADE, Md. – When Maj. Brooks Jarnagin, who is a Military Intelligence (MI) officer, graduated from the two-year Army Intelligence Development Program – Cyber (AIDP-Cyber) course in a ceremony at the National Cryptologic Museum here on June 1 he became a trend setter.

Previously, the graduates of the AIDP-Cyber program filled cyberspace team leader and other key and developmental (KD) positions within the fledgling Cyber branch; however, starting with Jarnagin, the focus has changed to providing cyber training and experience to MI officers who will be significantly ahead of their peers and become much more valuable to their tactical and strategic commands.

“When the (AIDP-Cyber) program was implemented we didn’t have a Cyber branch. It was originally designed to train MI or Signal officers to become Cyber officers,” said Lt. Col. Justin Considine, commander of the 781st Military Intelligence Battalion (Cyber) and the executive agent for AIDP-Cyber. “Now that we have a Cyber branch, we have a pipeline, a schoolhouse, and a Center of Excellence. We are now redesigning the program to produce cyber-savvy, operationally minded Military Intelligence officers to go back into the force and be better prepared to advise their commanders in FORSCOM (U.S. Army Forces Command) on how to integrate cyberspace effects into tactical operations.”

Considine said the two-year program is highly competitive and selects only the best and brightest MI officers. He went onto say that the AIDP-C graduates will stand head and shoulders above their peers when it comes to advising their commanders on cyberspace operations and planning cyberspace effects.

“I know when Brooks moves forward to be a brigade S2 (intelligence officer) he is going to feel the pressure to stay one to two steps ahead of his brigade commander. That is going to be a big challenge, because the commanders are being fed a lot of information about cyber, and sometimes they’re getting it more than their intelligence officer,” said Considine. “I have no doubt that Brooks is going to go into the force and he is going to have a significant advantage over the other brigade S2s, because he has been through this program. (He is) going to have the knowledge, the experience and the contacts.”

According to Lt. Col. Jesse Sandefer, the deputy commanding officer for the 780th Military Intelligence Brigade (Cyber), and the keynote speaker for the graduation ceremony, the MI branch allows only one to two MI officers a year to enter the AIDP-

officers

Cyber program.

"AIDP-C is intended to prepare officers to serve in positions requiring cyber leadership and planning expertise for the Army," said Sandefer. "It is a highly competitive program. So the simple fact that (Jarnagin) was selected for this program means we've already got a pretty damn good MI officer."

Once selected for the AIDP-Cyber, the MI officer is moved to Fort Meade, Maryland for a two-year program consisting of instruction from the National Cryptologic School, Department of Defense cyber-related courses, and through commercial information technology certification courses, followed by operational tours at the National Security Agency and U.S. Cyber Command.

Considine said two years has proven to be adequate time to conduct fundamental training in information technology, then to conduct three rotations, one focusing on offensive cyberspace operations (OCO), one on defensive cyberspace operations (DCO), and then one intended to be a capstone planning rotation, where the interns integrate their knowledge of cyberspace technologies and OCO and DCO into real world operations supporting the Cyber National Mission Force.

"It's a fire hose from the get-go," said Jarnagin. "You go through a lot of certification courses for the first three to four months -- A+, Net+, CSA+, CISSP (Certified Information Systems Security Professional) -- and then you start to transition out to different work centers, and once you complete your tour at those work centers you'll be trained in defensive cyber operations, offensive cyber operations and as a cyber planner."

Jarnagin calls himself a "Fort Bragg baby." He has been an MI officer since the beginning, serving six years with 4th Brigade, 82nd Airborne Division, including two operational tours, before attending the Captain's Career Course, then going back to the 82nd, where he deployed again. He also served two years at the Pentagon on the Headquarters, Department of the Army G-2 (Intelligence) staff as an executive officer.

***FORT GEORGE G. MEADE, Md.** – Maj. Brooks Jarnagin addresses the audience after graduating from the Army Intelligence Development Program – Cyber course in a ceremony at the National Cryptologic Museum on June 1. (U.S. Army Photo)*

It is a significant investment to have a high-caliber officer in training for that length of time, but Sandefer and Considine agreed the return on that investment is worth the time, for both the Cyber branch and the Army.

During the graduation ceremony Sandefer told Jarnagin to "Get assigned to some KD positions and influence the force, because we need smart Intel officers out there that can speak both SIGINT (signals intelligence) and cyber [and] CI (counterintelligence) and cyber, and if you do go on to be a brigade G-2 in the 82nd, the knowledge and experience you have gained here is going to do wonders both for that unit and for us, as we educate the Army."

Jarnagin had this advice for prospective MI officers who graduate from the program.

"I truly believe, and I think we all know this to be true, that cyber is just going to continue to grow in importance, and it's going to play a critical role in future conflicts," said Jarnagin. "So we in the MI Corps have to shoulder that task, shoulder that mission, and assume responsibility for that threat…so capture your lessons learned [and] get them back out to the MI community"

Army partners with UMBC to train tool developers for

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

***FORT GEORGE G. MEADE, Md. –** Spc. Grant Ward, a cybersecurity specialist from Southbury, Connecticut, assigned to the 781st Military Intelligence (MI) Battalion, 780th MI Brigade, was the 2018 Tool Developers Qualification Course distinguished honor graduate and received an Army Achievement Medal at a graduation ceremony in the post theater July 13. (U.S. Army Photo)*

"We must design, build, and deliver integrated capabilities for the future fight – spanning cyberspace, electronic warfare, and information operations. We must deliver capabilities to defeat adaptive adversaries that possess constantly changing tools and tradecraft." ***– Gen. Paul Nakasone, commander of U.S. Cyber Command.***

FORT GEORGE G. MEADE, Md. – The 780th Military Intelligence (MI) Brigade (Cyber) has partnered with the University of Maryland Baltimore College (UMBC) Training Center to design a Tool Developers Qualification Course (TDQC) which produces computer programmers for the U.S. Army and the fourth class graduated on July 13 at the post theater.

TDQC is an 11-month training program consisting of both formal classroom training and interactive class projects. The Soldiers enrolled in the program are tested at the completion of each of the 12 modules and are expected to achieve an 80 percent or better grade. Additionally, the Soldiers are required to complete a capstone project at the end of the course.

The goal behind the development of the TDQC was to design a progressive education curriculum where students were evaluated based upon how well they could complete individual programming assignments.

Col. Brian Vile, the commander of the 780th MI Brigade mentioned that out of the thousands of Soldiers in the 780th and 704th MI brigades the 12 TDQC graduates were joining only 56 others who had successfully completed this difficult path.

"TDQC is a critical step in building one of the Army's most specialized and critical positions – the tool developer," said Vile. "(TDQC graduates) are expected to operate independently on real world projects, to develop solutions to some of the most challenging problems in cyberspace."

According to the brigade S-3 (operations) training section, tool developers create, develop and code computer applications, software, or specialized utility programs. They conduct comprehensive technology research to evaluate potential vulnerabilities in cyberspace systems. Finally, they detect, identify and describe vulnerabilities to network devices and operating systems.

Spc. Grant Ward, a cybersecurity specialist from Southbury, Connecticut, assigned to the 781st MI Battalion, 780th MI Brigade, was the 2018 TDQC distinguished honor graduate.

"I didn't know a whole lot of programming before I started the course. TDQC taught me everything I needed to know," said Ward. "It was a great pace, really great teachers. The assignments are very challenging. They push you to become a better programmer."

Spc. Elijah Harmon, from Renton, Washington, assigned to the 741st MI Battalion, 704th MI Bde., was the 2018 TDQC honor graduate.

"When I enlisted, all I wanted to do was to be a developer," said Harmon. "The course taught me everything I thought it would teach me and more. Even if you don't know anything about computers, as long as you have the mindset of wanting to create, and disassemble, wanting to know how things work, tinker with stuff, then you are solid."

According to Sgt. 1st Class Joel Aguilar, brigade S-3, TDQC provides an education path for individuals to become experienced at 90 percent of the identified critical developer requirements an individual must be able to articulate and demonstrate through practical application in order to be certified as a Cyberspace Solution Engineer.

In his remarks to the graduating Soldiers, Vile congratulated the Soldiers for completing the course; however, he said it really was just the beginning.

"Today doesn't mark the completion of a journey, but rather the beginning of one. Graduation today is simply a milestone in what must become a longer challenging journey," said Vile. "This course has equipped you with the basics you will need to solve our most challenging problems in cyberspace, but how you use those skills to create solutions will ultimately be your greatest problem to solve."

2018 TDQC Graduates

Staff Sgt. Kirk David, C Co., 781st MI Bn.;

Sgt. Jonathan Goodman, E Co., 782nd MI Bn.;

Warrant Officer Jacob Harding, B Co., 781st MI Bn.;

Spc. Elijah Harmon, A Co., 742nd MI Bn.;

Spc. Devin Lee, Headquarters and Headquarters Co. (HHC), 780th MI Bde.;

Sgt. Jeffrey Lu, D Co., 781st MI Bn.;

Spc. William Marchant, E Co., 782nd MI Bn.;

Sgt. Nathaniel Muesing, A Co., 742nd MI Bn.;

Sgt. Christopher Pandoliano, D Co., 781st MI Bn.;

Spc. Mathew Reglein, B Co., 781st MI Bn.;

Sgt. Jiseng So, HHC, 781st MI Bn.;

Sgt. Aisha Umar, C Co., 781st MI Bn.; and

Spc. Grant Ward, C Co., 781st MI Bn.

Spc. Alexander Musarra
Bravo Co., 782nd MI Battalion (Cyber)
INSCOM Best Warrior

U.S. Army Photos

> *"The biggest challenge is juggling all the different things you need to be good at to do this. You can't just hit the gym. You can't just study. There are so many things while also managing things in life and work at my shop. That's the biggest challenge of this."*
>
> Spc. Alexander P. Musarra
> 35P Iraqi Arabic Cryptologic Linguist
> 782nd MI Battalion, 780th MI Brigade
> Fort Gordon, Georgia

FY 2019 NDAA UPDATE

By Maj. Timothy Minter, Command Judge Advocate, 780th Military Intelligence Brigade (Cyber)

Gen. Paul Nakasone, commander, U.S. Cyber Command (USCYBERCOM), noted that in order for USCYBERCOM to succeed in its mission, it will need to ensure that "we have the platforms, capabilities, and authorities ready and available to generate cyberspace outcomes when needed."

Congress appears to be looking to expand the Department of Defense's Title 10 authorities in H.R. 5515 - John S. McCain National Defense Authorization Act for Fiscal Year 2019 (FY2019 NDAA). As of the date of this writing, the FY2019 NDAA has passed both the House and Senate and is pending Presidential action. Sections 1621 – 1623 have several provisions that will be directly applicable to the Brigade's mission. The net effect of these provisions will be to extend our "Title 10" authorities.

First, the NDAA states that it is the "policy if the United States" to "employ all instruments of national power, including the use of offensive cyber capabilities" to deter and defend against cyber adversaries who threaten casualties, "disrupt democratic society" or "government (including government services," or threaten the command and control of the US military or civilian infrastructure the military relies upon.

Secondly, the NDAA gives SECDEF the authority – which he may delegate to U.S. Cyber Command – the authority to "develop, prepare, coordinate, and when appropriately authorized to do so, conduct military cyber activities in response to cyber-attacks and malicious cyber activities."

Thirdly, Congress has authorized the Secretary of Defense to conduct "operations in cyberspace, including clandestine military activities or operations in cyberspace" in response to malicious cyber activity against the US or US interests. These clandestine actions are defined to include the conduct of military activities or operations of cyberspace short of war and in areas outside named areas of conflict for the purpose of preparation of the environment, influence, force protection, and deterrence of hostilities, or counterterrorism operations involving the armed forces of the United States." These clandestine activities are considered traditional military activities (i.e., part of the Title 10 authority) but are nevertheless subject to Congressional oversight.

Fourthly, the NDAA authorizes Cyber Command, upon a finding by the National Command Authority that Russia is engaged in an active, systemic, and ongoing campaign of attacks against the Government or people of the U.S. in cyberspace, to take "appropriate and proportional action" in active defense and surveillance to "disrupt, defeat, and deter such attacks," which are again considered to be "traditional military activities."

If signed into law, the net effect of these draft provisions will be to increase the authorities under which DoD, US Cyber Command, and by extension, the 780th MI Brigade can have the "authorities to generate cyberspace outcomes when needed."

***FORT GEORGE G. MEADE, Md.** -- They (the adversary) know we exist," said Col. Brian Vile, commander of the 780th Military Intelligence Brigade (Cyber). "The brigade's Facebook page has 6,500 friends…over 4,000 of them are foreigners." (U.S. Army Photo)*

SHARP: Sustainable Readiness Is Possible

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

Sexual Assault and Sexual Harassment are readiness issues. Period. I am sure you have all heard that Readiness is the Army's #1 priority, but do you understand why SHARP is a readiness issue? Let me give you a little back ground first.

SHARP stands for Sexual Harassment/Assault Response and Prevention Program. In our Brigade, we are staffed with one full time Department of the Army Civilian Sexual Assault Response Coordinator (SARC – me!) and a borrowed full time military member (Sgt. 1st Class Morales) is the Brigade Victim Advocate (VA). I use the word borrowed because the person in that seat is on orders from the Brigade Commander for two to three years, and after the completion of their term, they return to their primary Military Occupational Specialty (MOS).

We have approximately 20 collateral duty victim advocates throughout our four geographically separated units. This number fluctuates due to PCS (Permanent Change of Station) in and out of our brigade, certification expiration, etcetera. These VAs are part time and only begin working for me when they are working with a victim on a case. Collateral duty victim advocates also provide training to the units and maintaining their own training through continuing education. So, we have a staff of around 22, not including the command teams and supervisors who also get involved in sexual harassment or sexual assault incidents.

So, how are SHARP and Readiness related?

When we have a SHARP violation in our unit, whether sexual harassment or sexual assault, everyone involved in the investigation—victim, subject, or witnesses—cannot deploy until the investigation is completed and possibly until it is adjudicated. A sexual assault that goes to court martial can take up to 18 to 24 months to be adjudicated. The process is lengthy partially due to there being only one lab that the Department of Defense uses for biological evidence, which is located in Atlanta. A formal sexual harassment case requires a full time Investigating Officer who gets pulled from their normal job and must concentrate solely on the investigation for its duration. The length of time for a sexual harassment case is typically much shorter and has strict timelines.

Taking care of the victim and ensuring safety, supporting the subject and ensuring they are cared for as well, speaking with Investigating Officers or CID and JAG—all takes time away from other issues the command teams could be handling—mission.

The victim of a SHARP incident needs to devote their time and energy to taking care of themselves and healing: emotionally, psychologically, and sometimes physically. They may also be involved in an investigation if there was an unrestricted report or a formal sexual harassment report. Their productivity may decrease, as their attention is diverted elsewhere. They may not be sleeping well at night due to nightmares and therefore may be tired. They may be withdrawn or angry. They may place blame on themselves, on the subject, and on the unit. There is a plethora of emotions a victim may be going through, and each and every victim responds differently to their unique situation.

Victims may feel they are alone; that no one supports them and they are going through the process on their own. We must all step forward and let them know they are not alone. It may be hard to relate to someone who has been a victim of sexual harassment or sexual assault if you haven't been through it yourself, but you can take the first step in supporting a victim by believing them.

So, are service members and civilians involved in a SHARP incident "Ready"? No. SHARP is directly a Readiness issue.

Only way for readiness to be sustainable is to prevent SHARP issues from happening by building a culture of dignity and respect and Bystander Intervention. When you don't step up and call someone out when they say something or do something off color -- out of the culture of dignity and respect -- you set a tone of acceptance. When that behavior is acceptable, we no longer have a culture of dignity and respect. When we are not continually building a culture of dignity and respect, we are no longer mission "ready". It is only by treating each other with dignity, fairness, and respect can we have sustainable readiness.

Prepared for the Mission

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

Readiness is an often discussed topic in the Army. Webster's defines readiness as the quality or state of being prepared mentally or physically for some experience or action. I would argue that being prepared both mentally AND physically are important as a Soldier or Civilian in our workforce. When it comes to Equal Opportunity and Equal Employment Opportunity in today's Army, discrimination in and amongst the ranks can lead to lack of mental readiness which in turn can impact an individual's physical readiness.

When an individual is discriminated against they can feel marginalized, and have any number of reactions. Some of these reactions can include retaliation, lowered work production, distancing themselves from their coworkers, and avoidance altogether just to name a few. Any of these would lead to a less positive work environment, and unit morale will decrease. This type of decrease in morale and work productivity can impact multiple people or even an entire work section. If a customer is relying on this work section to do its job, that customer is not paying the price for an act of discrimination that occurred on the other side of the globe. It may seem like a stretch, but just like any negative workplace experience it can have second and third order unintended effects.

In order for a person to be mental ready to conduct and support their Commander's mission, they must be in the right mindset free from undue stressors like discrimination and prejudice targeting them or others. Even bearing witness to an act of this nature can cause strife in a professional work setting. It is up to every person in the organization to respond appropriately and professionally when they witness an act of discrimination or targeted harassment. Many incidents that occur are not blatantly intentional acts that target others, and many people are not aware of their biases until they come out. When you observe something you know to not be right, or that could be perceived in a way that detracts from the good order and discipline of the unit, pull that person to the side and say something. Don't try to embarrass the individual, but be tactful and target the behavior displayed by the individual. Many issues can be resolved at the lowest level before they turn into complaints and destroy the morale of an individual or work section.

Once a month I encourage every person to experience another culture or a cultural event. It doesn't have to be anything extravagant and there are many free opportunities all the time. Most museums are free or have a very low cost to entry, and are a great way to experience and learn about other cultures at your own pace and to the extent you desire. Learning about other cultures is a great way to gain understanding of why people that are different from you may behave a certain way in certain situations. This too will help minimize acts of unconscious bias, and help sustain everyone's mental readiness in the work place.

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

- National Hispanic Heritage Month: 15 September – 15 October 2018
- National Disability Employment Awareness Month: October 2018
- National American Indian Heritage Month: November 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, Maryland. In addition, you can also contact your unit's Equal Opportunity Leader for assistance.

It happens in the best of marriages...

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

My wife and I will celebrate twenty years of marriage next spring. It has been a great two decades and we look forward to many more years together. However, it has not been without its struggles. We recently got into a brief argument over something minor. In the moment, however, it felt like a huge deal. If you are married, you know what I'm talking about. It happens in the best of marriages. Pride has a way of converting little offenses into major ones.

Later, I was still stewing inside and growing more irritated. I thought to myself: "She's always so … " But then I stopped before finishing the sentence in my head with a negative description. Instead, the words of a pastor and a friend filled my mind and heart, and changed my thinking.

The pastor who officiated our wedding once said to me: "Beware of global criticisms of your wife where you use words like 'always' and 'never.' They draw an unfair caricature of her and nothing good comes of it."

This advice has come back to me many times and stopped me from defining my wife in negative and unfair way. If I allow myself, in a moment of irritation or anger, to reduce her to one negative description, I eventually won't see her for who she is. I'll lose sight of her beauty and the qualities that make her unique. And what will I have gained? The agony of hanging on to an offense and allowing it grow, causing further damage is not worth the cheap and fleeting pleasure of winning an argument or feeling "right."

A friend of mine, who has been happily married to his wife for over fifty years, gave me similar advice on marriage: "Work on keeping a tender heart towards your spouse every day. Don't even let the thinnest sheet of ice cover your heart or it will eventually freeze over."

It is one thing to talk about keeping our hearts from freezing. It is another thing to actually keep the fires burning. For my wife and me, this has required learning to say "I'm sorry" along with a willingness to admit responsibility for an argument or offense. This is not always easy. It's the hard discipline of humility, deepened by the desire to build a lasting, solid and unbreakable bond in marriage.

Without this humility, our hearts would harden towards one another, making it difficult to love each other as we should. And I will say this, over time, it gets easier to swallow your pride and take the first steps towards reconciliation. When you see what a difference this can make and how it strengthens your marriage, it becomes easier to think less of yourself and more of your spouse.

And consider this, if I am taking these steps in times of struggle, and my wife is doing the same, we spend very little time in strife and much more time enjoying one another and building each other up. It is a win-win for both of us.

When I was single and people would tell me that marriage was hard, I didn't understand. I judged them, figuring they must not really love their spouse. Being married actually changed my mind. It is hard work. But worth every bit of effort and "humble pie" eaten along the way.

It takes commitment and determination to choose "we" over "me." However, the strongest marriages, the most enduring have recognized the importance of abandoning selfish pride for the sake of their spouse and the health of their marriage.

As the Bible says: "God has made everything beautiful for its own time" (Ecclesiastes 3:11). So for all of us married folks, let's take the time to do the hard work! If your marriage is struggling, determine today to love your spouse better. Abandon your pride more. Don't be so concerned with "winning" an argument, instead think of the long-term health of your union and the heart of your spouse. And for those of you looking to get married one day, tuck this advice away for the day you will need it, and look for a mate who not only loves you, but will remain committed to "doing the work" all of your days together.

Safety Tips for Heading Back to School

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

It is hard to believe that summer is almost over and the time to send the kids back to school is once again upon us.

Back to school time means it is also time to think about safety. Here are a few safety tips to help keep you and your children safe all school year long.

Riding the School Bus

- Make sure your child knows to stay seated while in the bus and that they use seatbelts when provided
- Make sure your kids wait for the bus to stop before approaching it from the curb and always remain in clear view of the bus driver

Backpack Safety

- Pack light. Organize the backpack to use all of its compartments. Pack heavier items closest to the center of the back. Backpacks that are too heavy can cause a lot of problems for kids, like back and shoulder pain, and poor posture. The backpack should never weigh more than 10 to 20 percent of the student's body weight
- Choose a backpack with wide, padded shoulder straps and a padded back •Make sure your kids always use both shoulder straps. Slinging a backpack over one shoulder can strain muscles

Bicycle Safety

- Whether child or adult, always wear a bicycle helmet, no matter how short or long the ride
- Ride on the right side of the road, in the same direction as auto traffic
- Know the "rules of the road." This includes no talking or texting on the phone while you are riding
- Use appropriate hand signals
- Respect traffic lights and stop signs
- Wear bright color clothing and a reflective vest to increase visibility

Walking to School

- Make sure your child's walk to a school is along a safe route and that your children cross streets only at marked crosswalks. Ensure they do not assume that they are completely safe in the crosswalk. Remind them to look in both directions, make eye contact with drivers, and ensure the vehicles are stopping before crossing
- Be realistic about your child's pedestrian skills. Because small children are impulsive and less cautious around traffic, carefully consider whether your child is ready to walk to school without adult supervision
- Finally, have your children were bright colored clothing. This will make them more visible to drivers

Drivers, Share the Road

- Don't block crosswalks
- Yield to pedestrians in crosswalks, and take extra care in school zones
- Never pass a vehicle stopped for pedestrians
- Never pass a bus loading or unloading children
- The area 10 feet around a school bus is the most dangerous for children; stop far enough back to allow them to safely enter and exit the bus
- Allow three feet when passing bicyclists...it's the law
- After passing a bicyclist, check over your shoulder to make sure you have allowed enough room before moving over

Why I Stay...In the Fight!

***SCHOFIELD BARRACKS, Hawaii** -- Sgt. Colin Pate (right), Detachment Hawaii, 782nd Military Intelligence (MI) Battalion, reenlisted in the U.S. Army in front of his detachment Soldiers as Lt. Col. Jason Hogan, the detachment commander, administered the Oath of Reenlistment and presided over the ceremony. (Courtesy photos)*

SCHOFIELD BARRACKS, Hawaii -- Sgt. Colin Pate, from Tacoma, Washington, a 35N, Signals Intelligence Analyst, assigned to Detachment Hawaii, 782nd Military Intelligence (MI) Battalion (Cyber), recently reenlisted in the U.S. Army.

Pate's future goals are to teach at the 35N schoolhouse and eventually become a 352N, Signals Intelligence Analyst Technical Warrant Officer.

His detachment was at his reenlistment ceremony, and Lt. Col. Jason Hogan, the detachment commander, was the reenlistment officiating officer.

When I found out that I was being assigned to Hawaii, and that I was going to be working a cyber mission, I was really excited. It has been a great experience so far, and I've added many new skills to my toolkit while being here. I'm looking forward to getting back to the MI Corps, so I can share the knowledge and expertise I've gained from the cyber mission. I love what I do for the Army, and want to stay in as long as I can. I also promised my previous First Sergeant, Master Sgt. (Promotable) Tyree Tucker, that I would be reenlisting shortly after I earned my stripes.

The people I work with every day helped to influence my decision to reenlist, particularly Staff Sgt. Bryan Wroda and Sgt. Gregory Mills. With the amount of knowledge they've passed down, and the time they've spent mentoring me, I feel obliged to pass down what I've been taught.

780th Military Intelligence Brigade Retention Team

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

781st Military Intelligence Battalion
Career Counselor
Sgt. 1st Class Soo Choi
Commercial: 301-833-6410

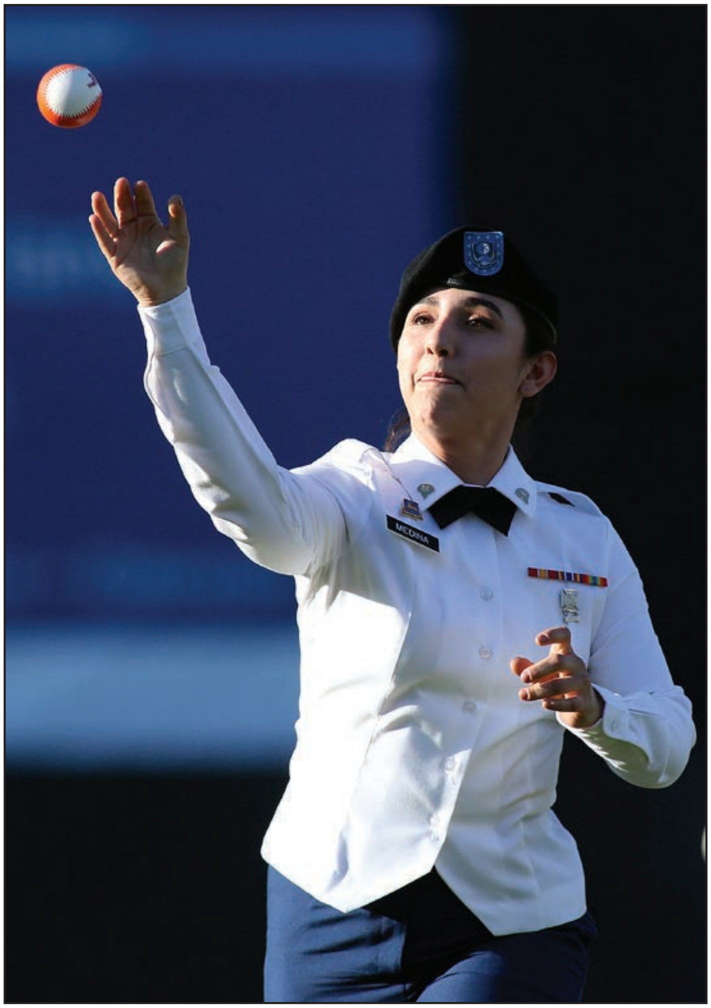
782nd Military Intelligence Battalion
Career Counselor
Sgt. 1st Class Michael Brothers
Commercial: 706-849-4789

ATLANTA – *Sgt. Mitchell Godfrey, a personnel support sergeant for the battalion S1 section, 782nd Military Intelligence Battalion (MI BN), reenlisted in the United States Army on the field at Sun Trust Park prior to the Atlanta Braves vs. Chicago Cubs baseball game on May 16. Throughout the month of May the Atlanta Braves organization recognized the Armed Forces, and although Godfrey is a die-hard Cubs fan, the organization went above and beyond to accommodate the noncommissioned officer's request to reenlist in front of his beloved Cubs. Capt. Kevin Jaworski, the company commander for Headquarters & Headquarters Company, 782nd MI BN (Cyber) is shown administering the oath to Godfrey in front of the fans and an eight-Soldier formation, including Godfrey's wife who is also a service member, and two flag bearers. (Photos by Cameron Hart/Beam Imagination/Atlanta Braves/ Getty Images)*

ODENTON, Md. -- *Master Sgt. Scott Morgan (right), the senior career counselor for the 780th Military Intelligence (MI) Brigade (Cyber), presents a farewell gift to Sgt. 1st Class Kevin Standring, the outgoing career counselor for the 781st MI Battalion (Cyber), on behalf of the Brigade at the All American Steakhouse, Aug. 9. (U.S. Army photo)*

Military Night scores home run with fans

By Cody Davis, Fort George G. Meade Sound Off!



BOWIE, Md. *-- Army Specialist Andrea Medina makes a throw during Fort Meade Night at Prince George's Stadium as the Bowie Baysox took on the Portland Sea Dogs on June 15. (Photo by Daniel Kucin Jr. For Baltimore Sun Media Group)*

BOWIE, Md. -- A succession of baseballs crossed home plate after two Fort Meade service members each threw the ceremonial first pitch before the Bowie Baysox took the field.

But neither was as astonishing as the bullet from Air Force Tech Sgt. Jason Hall of the Joint Force Headquarters, DoD Information Network, whose fastball drew gasps from the crowd.

The first pitches were part of "Fort Meade Night at the Bowie Baysox" on Friday evening at Prince George's Stadium.

Before their game against the Portland Sea Dogs, the Baysox kicked off the annual event with pregame festivities and recognition of military members and families.

"It's become kind of a tradition here for the Baysox," said Phil Wrye, the Baysox's assistant general manager. "We've been doing it for nine years now. … It's become part of what we do and it's one of the many military-themed events we do throughout the year."

Out on the field, Cadir, a 2-year-old Belgian Malinois, performed several tricks with his handler, Pfc. Brandon Dorthalina of the 2nd Military Working Dog Detachment.

The duo showed the crowd how they chase down a "bad guy" by demonstrating takedown tactics on Staff Sgt. Raymond Saxton, who was protected by a bite suit.

"We demonstrated the six phases of aggression," Saxton said later. "That's our patrol-side training using our dogs to apprehend a subject."

Saxton said Cadir is capable of apprehending or attacking fleeing subjects and detecting explosives.

After Cadir, who trained at Lackland Air Force Base in San Antonio, demonstrated his skills, the three service members took the mound for first pitches.

Lt. Col. Thomas Chapeau, commander of Headquarters Command Battalion, and Spc. Andrea Medina of the 782nd Military Intelligence Battalion stood alongside Hall, each waiting their turn.

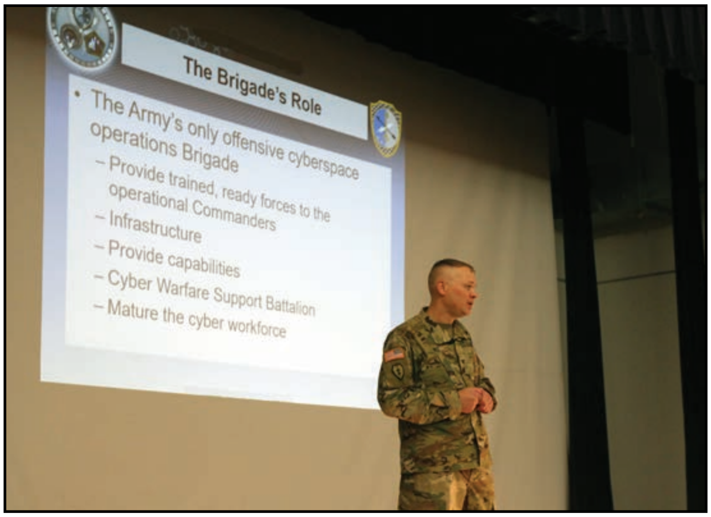
After the crowd applauded their efforts, the 704th MI Brigade Color Guard marched onto the field. As the color guard posted the colors, members of the Navy Cryptologic Warfare Group 6 Choir stood on the field to perform the national anthem.

During the seventh-inning stretch, the group also sang "God Bless America" and "Take Me Out to the Ball Game."

Navy Lt. j.g. Charity Jackson, the choir's leader, expressed enthusiasm at the event, saying later that most of the choir had not performed at a baseball game before.

Continued ⟶

Brigade Commander's Column (cont.)



The Brigade's Role

- The Army's only offensive cyberspace operations Brigade
  - Provide trained, ready forces to the operational Commanders
  - Infrastructure
  - Provide capabilities
  - Cyber Warfare Support Battalion
  - Mature the cyber workforce

FORT GEORGE G. MEADE, Md. *-- "It's pretty clear. First and foremost, I provide you. You are the nation's capability in cyberspace. This is the most expensive portion, this is the most important portion and this is the portion that can't be replicated," said Col. Brian Vile, commander of the 780th Military Intelligence Brigade (Cyber) (U.S. Army Photo)*

Continued from page 1

how these systems of systems work and interact, and being able to predict second- and third-order effects can only be done with an extensive knowledge of not only cyberspace, but of the real-world systems they support.

Through innovation, we will be well-postured to achieve our vision. The 780th will remain the Nation's greatest asset in cyberspace. Our adversaries will be deterred, understanding that we are a threat like no other they will face. And, when directed, we will be prepared to defeat our Nation's adversaries in and through cyberspace.

It is truly a humbling privilege to serve as your Commander, and I have no doubt that our team is up to this task.

Everywhere and Always, in the Fight!

Continued from previous page

Although the Baysox lost to the Sea Dogs, 2-1, the recognition made for a fun night.

"It's our honor to have everybody come on out and do these events," Wrye said. "It's our pleasure to offer this type of event and bring the [service] men and women and their families out here to have a fun time at a baseball game and enjoy themselves."

BALTIMORE *-- Garrison Commander Col. Tom Rickard and Spc. Angelo Camizzi of the 780th Military Intelligence Brigade, take a picture with the Oriole bird and Oriole Jace Peterson after throwing out the first pitch at Monday's Memorial Day game against the Nationals. (Nicole Munchel / Baltimore Sun Media Group)*

The Army is about opportunities and now this

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

FORT GEORGE G. MEADE, Md. *– Sgt. Marisa Tortolano, formerly a cyber Soldier assigned to the 780th Military Intelligence Brigade, became a West Point cadet on July 1 and will attend the United States Military Academy (USMA) because of her perseverance and by embodying the Warrior Ethos 'I Will Never Quit'. (U.S. Army photo)*

Sgt. Marisa Tortolano is from Bradenton, Florida and joined the U.S. Army in 2014 right after her high school graduation in order to support herself and because of the educational opportunities the military service could provide.

This fall, Tortolano will realize one of her education and career goals when she attends the United States Military Academy (USMA).

"I joined the Army because I knew I would be able to support myself and work while still going to school and getting the training to be successful in my field," said Tortolano. "Education was a big part of my decision."

When she initially signed her contract with the Army, Tortolano was a 35Q, Cryptologic Cyberspace Intelligence Collector/Analyst; however, she was transferred to the "new" 17C military occupational specialty, Cyber Operations Specialist, when the branch was created in October of 2015.

Tortolano joined the 780th Military Intelligence Brigade (Cyber) after her Advanced Individual Training and she gives credit to the officers she worked with for encouraging her to apply to USMA.

"I knew it was a huge opportunity to get my degree and commission through the most challenging program in the country," said Tortolano. "To give up that chance by not even trying just wasn't an option."

Although she was not accepted into West Point the first time she applied, Tortolano persevered (with a little push from her mentors and supervisors) because she wanted it badly enough.

"Maj. (Scott) Beal was the driving force behind getting me to reapply after that first failure," said Tortolano. "My biggest inspiration though was myself. This challenge will be greater than any I've taken on, but I can't wait for the feeling of accomplishment at the end. I've wanted to be an Army officer since I was in high school, and this is the most rewarding way I can think to accomplish that."

While the process she went through doesn't have a name, the West Point admissions page states Soldiers can be directly admitted to West Point; however, "One has to have a strong academic, leadership and physical background."

According to Beal she has these characteristics in spades.

"I saw in Marisa a drive and commitment to professional excellence that clearly placed her above her peers. Her poise…within the early days of the Joint Mission Operations Center (JMOC) as well as organizational management skills made her stand out to me," said Beal. "After several events with senior general and field grade officers, where she took the lead in briefing but also preparing the JMOC, I began to speak to her about her thoughts on leadership, the Army and the Officer Corps. Impressed, I began to encourage her to push herself beyond the traditional

Cyber Soldier is heading to West Point

FORT GEORGE G. MEADE, Md. – Sgt. Marisa Tortolano, a cyber operations specialist who was assigned to the 780th Military Intelligence Brigade, stands in the watch officer position of the Joint Mission Operations Center. (Army photo by Tina Miles)

career path of an NCO (non-commissioned officer) and OCS (officer candidate school) and to apply and re-apply for USMA."

"I think her time in the JMOC also showed her that persistence and will-power in attaining your goals and vision will pay off, not always the first time, but you see a problem, you attack it, and re-attack it if the outcome isn't the one desired," added Beal. "Marisa continued to attack the problem and reduced the obstacles placed in front of her. That is what we want in Army leaders and Army officers."

Tortolano plans on majoring in kinesiology or engineering and her goal is to branch aviation or cyber when she graduates.

"I have a feeling I'll be back in cyber at some point, (but) I hope to make the most of the next few years and take advantage of the internships and travel opportunities that are available," said Tortolano. "I want to serve my full 20 years, and train in physical therapy to work with wounded veterans."

Tortolano has this advice for her fellow Soldiers.

"I know most people groan when they think of MRT (Master Resilience Training) training, but resiliency has been super important in my own life," said Tortolano. "The lows will always come, but it's necessary, especially in this line of work, to make sure the highs happen too. The people around me and the resources available to me were key in getting me to where I am, I just had to realize it's okay to ask for help, that's how you grow."

"I know God put challenges in front of me and comrades beside me so I can continue through life even stronger than before," said Tortolano.

For more information on West Point and how Soldiers can apply, visit the West Point Admission page at https://www.usma.edu/admissions/SitePages/Home.aspx.

FORT GEORGE G. MEADE, Md. – Soldiers from the 781st Military Intelligence (MI) Battalion, 780th MI Brigade (Cyber), raised our Nation's flag at reveille in a time-honored military tradition, which was even more special to be a part of on a day we celebrated our country's independence -- the 4th of July. (U.S. Army photo)

780th Change of Command (cont.)

Continued from page 4

"He is the perfect selection for this command," said Johnston. "His war college fellowship at Carnegie Mellon, work at CyberCom (U.S. Cyber Command) to build operational models for the joint information environment, establishing the Army's first regional cyber center, and his cyber expertise will help shape the future of this unit as well as the Army."

It is always a bittersweet moment to say goodbye to a commander who has meant so much to the organization; however, knowing Col. Branch's next assignment is the executive officer for the commander of U.S. Army Cyber Command, Lieutenant General Stephen G. Fogarty, and that he will continue to have an impact on the brigade, is a blessing.

In his farewell remarks, Col. Branch thanked the team of Soldiers and Civilians, and his Family, especially his wife Lori, for their support.

In his remarks, Branch told the Soldiers, Civilians and Family members the story of Charles Plumb, a Naval aviator whose plane was shot down over Vietnam following his 75th combat mission. Plumb successfully ejected from his plane and was held captive by the North Vietnamese for more than six years. Years later, while he was at dinner with his wife, a man approached him and stated he had packed the parachute Plumb used after ejecting from his stricken aircraft, and it struck Plumb of the importance of teamwork.

"What this Brigade has accomplished, and what we will continue to achieve, requires and is reliant upon teamwork," said Branch. "I challenge myself and each of you today, to not lose sight of the fact that there are a great many Soldiers and Civilians figuratively 'packing our parachutes'. These fine men and women make our mission success possible. I am truly blessed to have served with each of you. Success is in your DNA. I look forward to seeing what this mighty brigade accomplishes next as it remains 'Everywhere and Always…In the Fight!'"

In addition to thanking Maj. Gen. Johnston and Lt. Gen Fogarty for the opportunity to lead the Soldiers and Civilians of the 780th, Vile said he wants to continue to move the organization forward as Branch has done.

"Dave, you've done an outstanding job moving the brigade forward and maturing the domain," said Vile. "And I can only hope to match your contributions to the force. Your impact on the 780th, the Army, and CyberCom, will be felt long into the future."

"Everywhere and Always…In the Fight!"

FORT GEORGE G. MEADE, Md. *– Maj. Gen. Gary Johnston (front right), commander of the U.S. Army Intelligence and Security Command (INSCOM), inspects the troops with Lt. Col. Jesse Sandefer (front left), the deputy commander of the 780th Military Intelligence (MI) Brigade (Cyber) and the commander of troops, Col. Dave Branch (back right), the outgoing commander of the 780th MI Brigade, and Col. Brian Vile, the new commander of the 780th MI, during a change of command ceremony hosted by on the McGlaclin Parade Field June 14. (U.S. Army Photo)*

“America’s pioneers” (cont.)

Continued from page 8

Considine’s departing message to his Soldiers and Civilians has been the philosophy he has embodied throughout his time in command – “Individual success is achieved through enabling the success of others. The success of the team should always come first. That is why the Army and our mission is so special – we do not fight for ourselves, but for a larger purpose.”

“My advice to the Soldiers and Civilians of the Vanguard, therefore, is to always remember that what makes us special is our commitment to defending the Constitution of the United States; to find patience and perspective in the fact that our current challenges and frustrations are temporary because we are a new force that is always evolving and improving; that identifying the problem is only the first step; that anything enduring and worthwhile takes time to build; and that helping to solve the problems we identify is what the Nation is asking of us and we cannot afford to let them down.”

Considine, and his family are not going far. His next assignment is attending the National War College of the United States on Fort Lesley J. McNair, Washington, D.C.

Lt. Col. Nally is not new to the Cyber Branch or the brigade. She was the team lead for 01 National Cyber Protection Team within the Cyber National Mission Force. Prior to this position, she served as the Military Assistant/Cyber Advisor to the Under Secretary of the Army; Chief of Staff to the Director of Net Assessment, Office of the Secretary of Defense; and a Strategic Planner for the Cyberspace Policy Division within the Joint Staff J5. Previously, she served as the operations officer of the 782nd MI Battalion (Cyber), a start-up unit she helped form from 20 to more than 450 personnel conducting full-spectrum cyberspace operations in support of joint force commanders.

“Your challenge lays before you, but I have no doubts that you are up to the task,” said Vile. “Your reputation precedes you, and you will continue to build this battalion to ever higher heights.”

Cyber teams to double (cont.)

Continued from page 6

“We weren’t a known entity to anyone,” one of the Soldiers said. The lesson learned was to integrate early into the operations planning process and attend home-station training prior to going to the combat training center.

Brig. Gen. William Hartman, deputy commander, Joint Force Headquarters, U.S. Army Cyber Command, looked back on the brief history of cyber. Just a few years ago a cyber team of four Soldiers was invited to their first combat training center rotation. There wasn’t Internet set up, so it was impossible to conduct realistic training.

On the next rotation, 35 cyber operators were able to surveil enemy targets at 900 meters, he said. On subsequent rotations, that improved to 5 kilometers, giving the maneuver commander the ability to see cyber activity around him from inside the tactical operations center.

Hartman noted that besides being really good at what they do, cyber operators need to know how to communicate to the maneuver commander and his staff in language they can understand.

Col. Paul T. Stanton, commander, Cyber Protection Brigade, oversees 20 cyber protection teams.

“We understand the ones and zeroes and the complexity of the systems we’re defending,” he said. “We develop interesting and novel algorithms, sometimes on the fly in order to analyze the data in a meaningful way to defend the network.”

Having said that, there are limitations to defending the network at the tactical edge, he noted. There are just 2 megabits of bandwidth per second available at the tactical edge, compared to many times that available at home station.

That means there’s limited bandwidth for those systems at the tactical edge, but the upside to that is there’s a smaller footprint, meaning it’s harder for the enemy to find and target the cyber team’s activities.

Battle of Trafalgar (cont.)

Continued from page 10

These lessons on readiness continue to apply to us today. Disregarding a sustainable state of readiness will push us until we run ourselves into the ground. Just as the French, my Company has seen the danger of this practice. Rebuilding is significantly more difficult than reserving the time necessary to maintain readiness. Similarly, our operational readiness becomes depleted if we are too slow to adopt new technology and abandon deprecated techniques. As leaders we must avoid the "sunk cost" fallacy and ensure we don't become too invested or complacent with ineffective training or operations objectives. Although we might not have to deal with scurvy, the French medical readiness pitfall is just as valid today. Cyber Soldiers may not need to be as fit as an Army Ranger, but constant medical appointments or a lack of sufficient physical fitness will eventually result in a noticeable reduction of combat power. Finally, as leaders (note: everyone is a leader) we must be competent in our specific craft. Being competent in our domain of battle is a prerequisite for training our forces in meaningful ways that result in increased lethality.

It is easy for us to focus on the pinnacle of battle. As Soldiers we are driven to mission accomplishment. Manning, training and planning all lead us towards mission execution. It is imperative that each Soldier understands how seemingly pointless tasks actually contribute to overall readiness and may culminate in mission impacts. A failure to do so may doom us in the day of battle as it did the Combined fleet at the Battle of Trafalgar.

Sustainable Readiness (cont.)

Continued from page 12

Next, our exercises must be conducted in a full spectrum environment with both offensive and defensive cyber elements operating in conjunction with each other on the same logical networks. The full spectrum fight requires additional training for Red Teams or opposing forces and the exercise development personnel in order to ensure they are able to build an effective attack and defense posture that is able to support the training needs.

Finally, we should begin to consider recertification exercises battle rhythm events that occur on a quarterly or semi-annual basis in order to continually refine and adapt our certification metrics to reflect the rapidly evolving battlefield.

Cyber Readiness (cont.)

Continued from page 15

network familiarization in AIT.

Currently, 35Q and 35N Soldiers with workroles identified as Target Digital Network Analyst (TDNA) and Digital Network Exploitation Analyst (DNEA) are the primary analytical backbone of the CMF, particularly within USCYBERCOM, but as the world's communications and critical infrastructure evolves, the lines between traditional Military Intelligence (MI) and Cyber are becoming increasingly blurred.

During a meet-and-greet with various NCOs of the 782D MI Battalion, the United States Army Intelligence Center of Excellence (USAICoE) Command Sergeant Major, Warren K. Robinson, was asked if the Army had any intent, or plan for relegating the 35Q digital network intelligence skills and responsibilities onto the 35Ns, and giving more cyber training than two weeks during AIT. He stated unequivocally that the mission of the MI corps was a tactical one, and would remain so. He is correct—as Secretary of the Army, the Honorable Mark T. Esper stated, "our Army remains the world's premier ground combat force and the bedrock of our Nation's defense." However, even in the furthest reaches of the world that our troops can deploy to, global communications standards evolve, and the Army needs to stand ready to bring tools and understanding of these new global standards to the battlefield. Therefore, additional cyber training is vital for ALL 35N Soldiers, and to an extent, all intelligence analysts.

In Afghanistan, where there was once barely a trace of a communications infrastructure, the Ministry of Communications and Information Technology (MCIT) evolved at a frantic pace since 2001. 17 years ago, at the dawn of the Global War on Terror, there were 35,000 phone lines, mostly landline, and many relied on radios. In 2018, there are seven mobile companies providing service to 18 million mobile customers, with increasing access to 4G and Very Small Aperture Terminals (VSATs), enabling a high level of mobile internet connectivity, and communications on countless virtual apps.

The MI Soldier is charged to "find, know, and never lose the enemy," and if the MI branch wishes to discharge faithfully in their sworn task, they absolutely must ensure that a robust and relevant understanding of basic cyber analysis is injected not only into SIGINT doctrine, but into all-source as well.

SANS curriculum developer Steven Winterfield wrote in 2001, "The US Army has made great efforts to automate the Intelligence Preparation of the Battlefield (IPB) process but has made little effort to apply IPB to the digital environment. The Army needs to develop this capability before it finds itself in a cyber war." Mr. Winterfield's prediction has come true, and the cyber war is here and now.

The cyber mission is not going to slow down, now or in the future. While the world may feel like it is getting smaller, the exponential growth of capabilities and the sheer vastness of the internet will prove perpetually challenging and elusive, and to truly ensure readiness, we must meet the challenge, grow, and evolve—both adaptively and rapidly.

Seizing the moment (cont.)

Continued from page 16

We have sync meetings and peer-level, work role training to discuss what we are doing and how we approach performing our duties. Not only are these a good way to keep up with everyone's contributions, but they also allow us to get fresh eyes and new insights into our work. They are an excellent opportunity to share lessons learned and best practices. They allow us to better understand how our efforts fit within the larger mission, which allows us to feed each other better information to produce a better result. This makes everyone on the team more capable and experienced in their own work roles and as members of the team, which in turn makes us all more ready to take on whatever may come.

But this is the Army. No one stays in one place forever. When experienced Soldiers leave and new Soldiers replace them, there's a dip in performance readiness as a new Soldier learns the job, the tools, and the routines to be successful. That's why we write SOPs (standard operating procedures). A good SOP, which explains the routines and responsibilities of a task or job, is a short cut, allowing new members of the team to pick up speed faster and become mission-ready sooner.

It is important to remember that SOPs are also living documents. We should update them regularly. Everything we do to keep ready, those best practices, those reliable battle rhythms should all be documented. If someone gives you a useful tip which will help you do your job better, ask if it is documented anywhere. Is there a place for it in the SOP? If there is, put it there so that nugget of wisdom does not disappear when you both leave the unit. Without an SOP to preserve the experience, insight, and 'best practice' advice -- we hurt our readiness tremendously with every PCS.

Sustainable readiness is not just some buzzword. It is an easily achievable goal. If we stay on top of our battle rhythm tasks, share our lessons learned both in person and in writing, ask questions, and practice what we know, there is no reason we can't face any challenge from "Anyone. Anywhere. Anytime".

Adopt a School (cont.)

Continued from page 18

Principal Craig Baker renewed their contract to continue supporting the Adopt-A-School Program.

Stephanie Bryant with the U.S. Navy said it quite well, "It's very important for the military to get involved with the youth of today because they're so many temptations and teachers are spread so thin, so if we can support the school systems and help our kids from every walk of life do better in the future we're building a better society." There are many ways to go about supporting your community; but one of the best ways to support is the future youth. These children are the future, and while not every child will make the choice to join the military; they may one day be the doctors, lawyers, teachers or cybersecurity experts we depend on to make a difference in this great nation. There is no better feeling than to know that you helped guide and mentor them into working towards their goals and watching them succeed.

FORT A.P. HILL, Va. – Spc. Alexander P. Musarra, assigned to the 782nd Military Intelligence (MI) Battalion, 780th MI Brigade, runs up a log to get over an obstacle at the 2018 INSCOM Best Warrior Competition, Fort A.P. Hill, Virginia, June 27. (U.S. Army photo by Jocelyn Broussard)