Volume 6, Issue 4

the BYTE

780th Military Intelligence Brigade

* Cyber Blitz 2018
* Army Cyber Skills Challenge VI
* Brigade Senior Leaders Week
* We are the Praetorians!

Army Cyber Vision

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...

Photos

On the cover: ***JOINT BASE MCGUIRE-DIX-LAKEHURST, N.J.*** – *Spc. Daniel Pappas, a member of the Expeditionary Cyber Support Detachment, 782nd Military Intelligence (MI) Battalion, 780th MI Brigade (Cyber), supports Cyber Blitz 2018 in order to test Cyber Electromagnetic Activities, or CEMA, concepts for the Army. (US Army Photo)*

Features

Articles

From the Editor

The theme for this issue is *"The Army Cyber Vision."*

In support of the Army and U.S. Army Cyber Command vision statements, Col. Brian Vile, commander of the 780th Military Intelligence (MI) Brigade (Cyber), presented the Brigade's vision to the organization's Soldiers and Civilians in a series of town halls and during the Brigade Senior Leaders Week in November when he declared "We are America's most innovative cyberspace operations force, deterring, and when directed, defeating our nation's adversaries in and through cyberspace."

In this issue of the BYTE we address how the brigade plans to achieve the objectives spelled out in the Army, ARCYBER, and Brigade vision statements.

Additionally, at the Brigade Senior Leaders Week, Col. Vile and Command Sgt. Maj. Krog announced we are the "Praetorians", joining the "Vanguard" of the 781st MI Battalion (Cyber) and the "Legion" of the 782nd MI Battalion (Cyber).

"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 2018 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.

'80MIB QRCode.png

Deterrence is an essential element of the DoD mission

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

Deterrence is an essential element of the Department of Defense's mission and a pillar of our Nation's National Defense Strategy. Within these foundations, the Cyber Mission Force has an essential role to play. By building and maintaining a credible capability within cyberspace, the Brigade plays a critical role in deterring our adversaries.

Deterrence is well defined; according to the DoD Dictionary, deterrence is, "[t]he prevention of action by the existence of a credible threat of unacceptable counteraction and/or belief that the cost of action outweighs the perceived benefit." Deterrence calculus is simple on its face; an adversary is deterred when perceived benefits are less than the costs of both executing the attack and the perceived consequences.

AN ATTACK IS DETERRED WHEN

PERCEIVED BENEFIT < **COST OF ATTACK** + **CONSEQUENCES**

Although the concept of deterrence is plain, the underlying considerations across diplomatic, informational, military, and economic elements are exceedingly complex. As our adversaries go through their decision-making process, they make every effort to reduce uncertainty. A key part of this process is ensuring that both attack costs and consequences are quantifiable.

In traditional warfare, military costs and consequences are relatively easy to estimate. Intelligence efforts have well documented both U.S. and adversary conventional capabilities. Anyone can use Wikipedia to estimate the size of any nation's air, land, and maritime forces and the capabilities and quantities of the associated weapons systems.

Traditional military capabilities are, in Donald Rumsfeld's words, "known knowns, ... things we know we know." These "known knowns" have enabled deterrence in the traditional domains for centuries. There are also "unknown unknowns" (such as highly classified and unacknowledged capabilities), but the hidden nature of these facts prevent them from impacting deterrence.

The advent of cyberspace has affected deterrence by upending both cost and consequence calculations. First, the cost of resourcing cyber-attacks is low; the tools necessary to engage in cyberspace are widely available on the web for download. For those lacking technical inclination, hackers for hire provide other options. Second, a lack of clearly defined norms in cyberspace allows our adversaries to act with less concern for consequences, including military consequences. Third, attribution can be difficult. Even with attribution, a lack of precedent complicates near-term response options. The low costs and ill-defined consequences of cyber-attacks result in the perception that the benefits of intellectual theft, destructive, or corrosive attack through cyberspace almost always make it worthwhile.

Our offensive capabilities, a "known unknown" to our adversaries, stand ready to provide consequences.

USCYBERCOM allows the United States to add intractable complexity to our adversaries' deterrence calculus and help prevent attacks before they occur. Our defensive cyberspace operations capabilities, whether internal measures or responsive in nature, increase the cost of staging a successful attack. Our offensive capabilities, a "known unknown" to our adversaries, stand ready to provide consequences. The operational security associated with offensive cyber ensures our adversaries will be unable to definitively estimate the consequences of an attack, making them uncertain in their ability to achieve a worthwhile benefit.

Continued on page 39

The Army Cyber Vision: The key is the Soldier

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

This quarter's theme is "The Army Cyber Vision." To fully articulate where we fit in the Army Cyber Vision, you first need to know what the vision statements are for the Army, U.S. Army Cyber Command (ARCYBER), and the Brigade.

The U.S. Army Vision: "*The Army of 2028 will be ready to deploy, fight, and win decisively against any adversary, anytime and anywhere, in a joint, multi-domain, high-intensity conflict, while simultaneously deterring others and maintaining its ability to conduct irregular warfare. The Army will do this through the employment of modern manned and unmanned ground combat vehicles, aircraft, sustainment systems, and weapons, coupled with robust combined arms formations and tactics based on a modern warfighting doctrine and centered on exceptional Leaders and Soldiers of unmatched lethality.*"

The ARCYBER Vision: "*A force that can aggressively operate and defend our networks, data, and weapons systems; A force which delivers effects against our adversaries in and through cyberspace to enable commanders' objectives; A force that designs, builds, and delivers integrated capabilities for the future fight – spanning cyberspace, electronic warfare and information operations. We do this by developing our people, improving our processes, and building partnerships.*"

The 780th Military Intelligence Brigade (Cyber) Vision: "*We are America's most innovative cyberspace operations force, deterring, and when directed, defeating our nation's adversaries in and through cyberspace.*"

The key concept in all of these is the Soldier. Without trained and ready Soldiers, we would not be able to accomplish any of these visions. The key to this is trained and ready. The Army's new non-deployable policy will help with the readiness by increasing the Army's deployable rate. Where we can help the most is training. The training pipelines for our work roles takes too long to complete. Some claim this is due to course availability, but when there are over 200 open Army seats in training it is hard to believe that availability is the key issue. We need to take every opportunity to train our Soldiers in their assigned work roles in as short a time as possible. Failure to do so shows a lack of regard in taking care of our Soldiers.

In reality, it is costing our Soldiers money. Every Soldier trained and certified in an ARCYBER work role is authorized to receive assignment incentive pay, and on the enlisted side they are authorized special duty assignment pay. The longer it takes to train our Soldiers affects their ability to receive these incentives. It also affects their ability to achieve the desired endstates of the visions stated above and their ability to accomplish the mission to the fullest extent. Each person on the team should be a fully trained and contributing member of the team. If not, then the team is not functioning to its fullest capability. It takes exceptional leaders to sacrifice now to develop the exceptional Soldiers, Civilians, and leaders of the future. We have an exceptionally smart and talented workforce. If we fail to fully develop them, we are not taking full advantage of their capabilities. We must develop our personnel now so that we are the capable force that achieves the endstates described in the Army, ARCYBER, and Brigade Vision statements. We must be the innovative, agile, and adaptive cyber force of the present and the future – ready to engage and defeat any adversary, anytime and anywhere through the use of capabilities our teams have developed to cause cyber effects in support of the warfighter, Combatant Commands, and nation.

While we may be ***"Everywhere and Always…In the Fight!"***, we still must ensure our ability to continue to do so in the future. We can only do this by ensuring our personnel are trained and ready to meet the requirements of the nation as depicted in the Army, ARCYBER, and Brigade Vision statements.

A Nibble on Leadership

By Chief Warrant Officer 5 Travis Ysen, Senior Technical Advisor, 780th Military Intelligence Brigade (Cyber)

The replacement of Presidential Policy Directive 20 with National Security Presidential Memorandum 13 serves as an open call to all members of the 780th Military Intelligence Brigade (MI BDE) to break through the constraints of how things are, and be actively engaged in the design of how a cyber brigade could and should be. Now, more than ever, the Cyber Mission Force needs leaders within its workforce to develop innovative solutions to complex problem sets that will provide advantage and hold the adversary at risk.

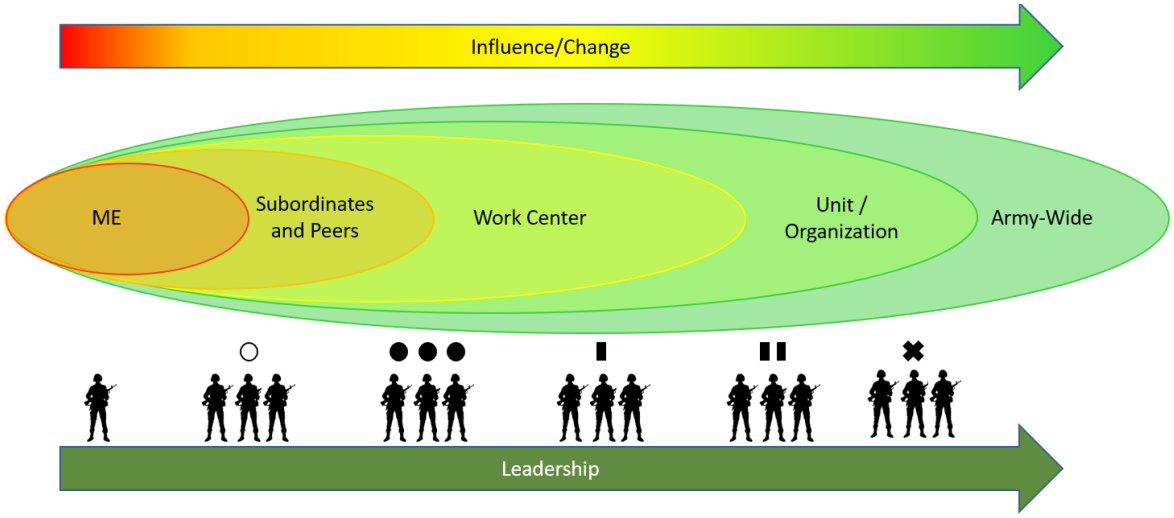
I remember as a young Staff Sergeant thinking that leadership had little to no place in the daily execution of my mission as a signals analyst. Signals analysis mirrors cyber in that it is highly technical and requires vast amounts of focus, research, and persistence to attain success. A great amount of pride and self-worth is derived from solving complex signal structures in support of strategic, national, and tactical objectives. Any distraction from mission execution, normally attributed to leadership, was looked upon in a negative light.

At the time, I readily recognized leadership as being a function of squad leaders, platoon sergeants, first sergeants, and commanders primarily charged with the administrative management of personnel. Based on my finite understanding of leadership, my desire to build technical competence, and dedication to the operational mission left me with little interest in becoming a leader at the time. What I failed to realize was that leadership spans a wide gradient that not only includes the aforementioned positions, but also extends to individual efforts within a work center and unit. Examination of the Army's definition of a leader and leadership in Army Doctrine Publication 6-22 (Leadership) further exposes shortcomings of my narrow view.

> ***An Army leader is anyone who by virtue of assumed role or assigned responsibility inspires and influences people to accomplish organizational goals. Army leaders motivate people both inside and outside the chain of command to pursue actions, focus thinking and shape decisions for the greater good of the organization.***

Leadership is the process of influencing people by providing purpose, direction, and motivation to accomplish the mission and improve the organization.

Leadership, in its simplest form, involves at least two people or groups working in cooperation with each



other. This, in combination with these empowering definitions, opens the aperture beyond the scope that I understood as a junior Non-Commissioned Officer. When applied to an organization that pursues technical competence and operational mission accomplishment over all other objectives, the terms leader and leadership take on a much more palatable connotation.

Each person, regardless of their role, has an opportunity to be a leader, even in a technical organization like the 780th MI BDE. Leadership hinges on an individual's conscientious choice to apply their time, energy, and talent to improve the mission. In a technical environment, leadership requires extensive self-development and continuous learning coupled with the training and mentorship of subordinates and peers. An individual that functions in this capacity, a leader, will be well positioned to inform high-level decision makers, drive innovative thought and actions that result in cutting edge capabilities, streamline processes, update policy, and improve competence across the workforce.

As with leadership, innovation and change can be initialized from anywhere, by anyone. This concept is not new, but requires patience, persistence, and coordination down to the individual level to be successful. To be clear, change is not something that occurs overnight, but is a prolonged effort that is not deterred by failures or setbacks. Oftentimes, this is easier said than done as motivation and interest can wane as resistance mounts or challenges arise. However, the more an individual proactively engages in the leadership process throughout their career, the greater influence they will have on mission improvement and change despite any challenges that occur. A key point to this is realizing that we are not victims of the system. Rather, we are talented members, leaders, within a larger team whom can influence change, drive innovation, and improve the mission. In short, stay in the fight, let your voice be heard, you can make a difference – we need you now more than ever.

Sources:

Army Doctrine Publication (ADP) 6-22, Army Leadership, dated Aug. 2012

White House authorizes 'offensive cyber operations' to deter foreign adversaries, by Ellen Nakashima, Washington Post, September 20, 2018.

Praetorians

The Praetorian Guards were an elite unit of the Roman army and included hand-picked veterans from the Roman legions.

The Praetorian Guard became notable for its intrigue and interference in Roman politics. Just as the 780th Military Intelligence Brigade (Cyber) is the elite protector of the nation, the Praetorians were the protector of the Empire and Roman emperor.

The Soldiers and Army Civilians of the 780th Military Intelligence Brigade (Cyber) are the nation's "Praetorians", the royal guard of the cyber domain. We operate in gray and red space and are the nation's preeminent cyber force.

The Praetorians augment and support the "Vanguard" of the 781st Military Intelligence Battalion (Cyber) and the "Legion" of the 782nd Military Intelligence Battalion (Cyber).

Our message to our nation's adversaries is we are "Everywhere and Always…In the Fight!". We are the Praetorians!

Vanguard: "Getting back to basics..."

By Lt. Col. Nadine Nally, commander, 781st Military Intelligence Battalion (Cyber)

The leaves are starting to fall from the trees, the battalion has completed its fall APFT (Army Physical Fitness Test) week, Command Sgt. Major (Jesse) Potter added another Spartan race with accompanying bling to his logbook, and Killian is now six months old. It's hard to believe that it's been three months since I took the guideon! Throughout my first quarter in command I've heeded the advice every mentor has given every new commander – observe first, change second. My observations have been mostly positive – Vanguards participated in Cyber Blitz and AVENGERCON, conducted a Quarterly Training Brief (QTB), reenlisted 18 Soldiers, re-task organized, welcomed new commanders, and held several professional development sessions – all great things! However, I also observed a few areas where we need a little rudder-steer: organizational culture.

Our junior officer & noncommissioned officer (NCO) force has been busy developing the technical skills that they view as defining characteristics of leaders while our mid-range officers and NCOs are leveraging operational experiences gained from GWOT (Global War on Terror) and COIN (counter-insurgency) to lead, train, and mentor our Soldiers. Unfortunately, I believe a gap has inadvertently developed and is widening between our junior/mid-range leaders and the Army's core culture. As a result, I've witnessed discouragement, attrition, and the loss of a shared vision.

A deliberate plan is needed to get after this. My goal is to conduct leader professional development sessions focused on getting us back to basics. We need to re-learn the Army's eight-step training model, post T+6 training (lock in training six weeks out) calendars, submit training forecasts, and understand how to properly plan, resource, and execute training. Moreover, we need to be able to do this in a resource constrained environment. This will enable us to provide predictability to our Families, our Soldiers, and our OPCON (operational control) mission partners.

Addressing shortfalls in our understanding of training and resourcing only solves part of the problem. We also need to be vigilant leaders (not managers). The uniform on our backs and patch on our shoulders both bind us and separates us from our counterparts in corporate America. We have an obligation to watch out for our battle buddies, to keep them safe and alert others when we think someone needs help – we are all scouts and we need to close ranks on Soldiers who need our help! As we enter the holiday season I ask that you remain vigilant against those who wish to harm us and our communities, stay keenly attuned to indicators and warnings that a fellow Soldier or Civilian may need help, and finally take time this holiday season to reflect on the many blessings that we enjoy – our loved ones, our freedoms as Americans, and the privilege of serving our great Nation. Given the demands of our work, we too often get caught up in the pace of everyday life and don't take time to appreciate just how fortunate we are.

We got this!

"Vanguard...When Others Cannot!"

FORT GEORGE G. MEADE, Md. *– Lt. Col. Nadine Nally and Command Sgt. Maj. Jesse Potter, the senior leaders for the 781st Military Intelligence Battalion (Cyber), took part in the military's tradition of 'serving those who serve', on Thanksgiving day at the Freedom Inn dining facility. (U.S. Army Photo)*

Cyber Legion: "The deterrence value"

By Lt. Col. Jason R. Sabovich, executive officer, 782nd Military Intelligence Battalion (Cyber)

The United States Army today is without question the most lethal force ever fielded by the Nation. The ability of the Army to fight and win our Nations wars at the strategic level gets at the very essence of its existence. Arguably as important as the capability of defeating our enemies on the battlefield, is our capacity to deter our Nations enemies from waging war. This is highlighted by General Milley and the honorable Mr. Esper in the Army Vision Statement for 2018, which states "The Army of 2028 will be ready to deploy, fight, and win decisively against any adversary, anytime and anywhere, in a joint, multi-domain, high-intensity conflict, while simultaneously deterring others and maintaining its ability to conduct irregular warfare." In regard to the deterring element, the U.S. Army and our Nations Joint cyberspace forces have a long way to go before they are seen as a credible deterrent.

The deterrence value of the Nation's armed forces is determined by an adversary's perception of our combat effectiveness and our willingness to use force. In high intensity conflict, the U.S. Army in concert with joint forces, demonstrated absolute dominance in Operation Desert Shield / Desert Storm in 1990/1991 as well as Operation Iraqi Freedom in 2003. As a result, there is arguably no military on the planet that is willing to engage the U.S. Army in conventional battle. This is precisely because there is ample evidence that destruction awaits any challenger. The deterrence value this provides cannot be overstated.

A similar level of deterrence does not exist in cyberspace for the Army. The barriers to entry to engage in offensive cyberspace operations are very low, combined with the relative ease of obfuscating one's true identity. The result is that the challengers to our Nation's national security in cyberspace are vast, and potentially encompass anyone with an internet connection and the will to do harm. Against this backdrop, offensive cyberspace operations carried out by the U.S. Army are rightly constrained by U.S. law and tight control.

Another significant factor that is difficult to overcome in regards to deterrence in cyberspace is the requirement for secrecy. When the U.S. Army engages in ground combat operations, there is no question to the enemy who they are fighting; the uniforms and equipment make that apparent. In offensive cyberspace operations, if you are found at all, then it is generally simple for a competent system administrator to stop even very capable cyberspace operators. The objective becomes: deliver effects and never let the enemy find you.

There are no easy solutions to addressing this problem, however, that is not to say the U.S. Army is without effective options. Most important is that these options demonstrate to our adversaries that the United States possesses the capability of delivery overwhelming firepower in cyberspace AND the willingness to use that firepower if provoked. There is no doubt that the U.S. Army of 2028 will deliver.

Special thanks to the Battalion Civilian Personnel Office and Resource Management Office, including: Mrs. Carrillo, Mrs. Sweitzer, Mrs. Frazier, Mrs. Shoffner and Mrs. Alford, who enable much of the behind the scenes success of the Battalion.

The Cyber Legion continues answer the call of the nation in cyberspace. The men and women of the 782D Military Intelligence Battalion continue increasingly push the boundaries of offensive cyberspace operations to the detriment of our Nations foes. We remain as always "Everywhere and Always … In the Fight."

"Cyber Legion...Silent Victory!"

Army Cyber Skills Challenge: Identifying the Army's

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

***SCHOFIELD BARRACKS, Hawaii** – The physical and tactical portion of the 6th annual Army Cyber Skills Challenge, hosted by the 780th Military Intelligence Brigade (Cyber), began with a modified Army Physical Fitness Test, followed by a 6.2 mile road march, the Army Combat Readiness Test, four of the Army Warrior Tasks, and a day land navigation course, with competitors participating in the first part of the challenge from Fort Meade, Md.; Fort Gordon, Ga.; Schofield Barracks, Hawaii; and Joint Base San Antonio, Texas. (U.S. Army Photo)*

FORT GEORGE G. MEADE, Md. – Soldiers and Army Civilians from the U.S. Army Cyber School, Army Cyber Command, the Cyber Protection Brigade, 704th Military Intelligence (MI) Brigade, and the 780th MI Brigade (Cyber), competed in the 6th annual Army Cyber Skills Challenge (ACSC VI) for the honor of being named the best Cyberspace Warrior on November 16.

Competitors participated in the three-day ACSC VI event, simultaneously, at Fort Gordon, Ga., Schofield Barracks, Hawaii, Fort Meade, Md., and Joint Base San Antonio, Texas.

The physical portion of the competition began on Nov. 14 with a modified Army Physical Fitness Test, followed by a 6.2 mile road march, the Army Combat Readiness Test, four Army Warrior Tasks, and a day land navigation course. The 24-hour technical portion of the event, which tested the participants' cyberspace skills, began on November 15th through midday on the 16th, and was followed by the award ceremony recognizing the top competitors from the physical and tactical portion, the technical portion, and the overall best cyber warrior.

According to event organizers, there were more than 100 competitors participating in this year's cyber challenge, doubling the field from last year and the first time Soldiers and Civilians competed from Texas.

"ACSC is a competition to truly test the overall Cyber Soldier concept, not just the nerd, but the Soldier too," said Chief Warrant Officer 4 Troy Ward, the technical director for the Joint Military Operations Center and one of the ACSC event organizers. "It's important for our Soldiers, and the Army overall, to know that our guys can still deploy anywhere, anytime and be able to perform the same basic tasks that are expected of everyone else in the Army. The part that I found very interesting was the scores for the Army Combat Readiness Test portion of the physical event. Everyone who competed passed with at least 60 points in each event tested (based on the draft standards Army Times has published)."

The ACSC VI Physical and Tactical event champion is Sgt. Lance Pace from Detachment Hawaii, 782nd MI Battalion (Cyber), and the Technical event champion is Sgt. Jonathan Haubrich, 782nd MI Battalion (Cyber), Fort Gordon. This year's Best Cyberspace Warrior is Sgt. Jonathan Haubrich, a cyberspace operations specialist (17C) from Bellmawr, New Jersey.

***FORT GEORGE G. MEADE, Md.** – Soldiers competed in a 6.2 mile road march as part of the physical portion of the 6th annual Army Cyber Skills Challenge on November 14. (U.S. Army Photo)*

top cyber warriors

"Competing in ACSC was an incredible opportunity to put my skills and knowledge to the test. It was also a great opportunity to hack away in a room full of like-minded people," said Haubrich. "I have never gone to a live CTF (capture the flag) or anything similar in the past, and the experience was awesome!"

Ward said the 24-hour technical portion tested the competitors on a variety of topics from forensics, to reverse engineering, to cryptography. The challenges ranged from entry level to highly advanced. He stated more than 1,400 flags were captured over the course of the competition.

FORT GEORGE G. MEADE, Md. *– Soldiers competed in a day land navigation course as part of the physical portion of the 6th annual Army Cyber Skills Challenge on November 14. (U.S. Army COMCAM Photo)*

Haubrich's advice for future competitors?

"In general, stay hungry," said Haubrich. "Learn to love the work, and never stop learning. For ACSC, preparation is key – Exercise, read the regulations, and practice, practice, practice."

Because the ACSC competition is geographically dispersed throughout the United States – in Georgia, Hawaii, Maryland, and Texas – event organizers hope to entice participants from throughout the U.S. Army, active, National Guard, and Army Reserve, and are working toward the goal of not only crowning the best Army Cyberspace Warrior, but it becoming a recognized badge for Cyberspace, Electronic Warfare, and IT-affiliated Soldiers.

FORT GORDON, Ga. *– The 24-hour technical portion of the event, which tested the participants' cyberspace skills, began on November 15th followed by the award ceremony recognizing the top competitors. (U.S. Army Photo)*

Col. Brian Vile, the commander of 780th MI Brigade, foresees the competition growing into an equivalent of other MOS-specific badges such as the Expert Infantryman Badge and the Expert Field Medical Badge. "EIB and EFMB are recognized across the Army as a mark of excellence. Cyber, like the Infantry and medical communities, requires a mark to identify the top-tier talent that has demonstrated an ability to perform above the standard in both the land and cyber domains."

FORT GEORGE G. MEADE, Md. *– The 24-hour technical portion of the event, which tested the participants' cyberspace skills, began on November 15th followed by the award ceremony recognizing the top competitors. (U.S. Army Photo)*

CYBER SNAPSHOT: Sgt. Jonathan Haubrich

780th Military Intelligence Brigade (Cyber)

SNAPSHOT: Sgt. Jonathan Haubrich

Cyber Operations Specialist (MOS 17C)

A Company, 782nd Military Intelligence (MI) Battalion (Cyber), Fort Gordon, Ga.

Hometown: Bellmawr, New Jersey

QUICK SKETCH:

-- Overall champion of the 6th annual Army Cyber Skills Challenge (ACSC)

-- Works in the Cyber Solutions Development (CSD) Detachment at Fort Gordon

-- Wants to attain a computer science degree through the Army's Green to Gold program

ON PREPARING FOR ACSC:

"The Cyber work roles are technically demanding, so, fortunately, I get to experience and solve problems that are similar to those in ACSC every day. In my free time, I enjoy reverse engineering and vulnerability research, and those skills were very useful for the harder problems in ACSC. In addition, the 782nd MI Battalion has provided me with so many training opportunities. Recently, I took Penetration Testing with Kali (PWK) to prepare for the Offensive Security Certified Professional exam. The knowledge from PWK and practicing on hackerrank.com helped me become familiar with many of the problem types presented in ACSC."

ON JOINING AND STAYING CYBER IN THE ARMY:

"I joined the Army because of the opportunities it provides. The Army offers opportunities for education, travel, and most importantly personal growth. I would not be who I am today without the experiences I have had in the Army. 17C is actually my third MOS, and I chose it because I am passionate about learning as much as I am about computers. Growing up, I was always fascinated by viruses, cracking, and programming. I never imagined I would work in a place like the 782nd MI Battalion where I am surrounded by those things on a daily basis."

ON FUTURE GOALS:

"I want to do whatever I can to become a better tool developer and to continue contributing to the Army's Cyber mission. In particular, I am hopeful I will be afforded the opportunity to complete my computer science degree through the Army's Green to Gold program, and further down the road I would love to participate in the Computer Network Operations Development Program."

***FORT GORDON, Ga.** – Sgt. Jonathan Haubrich was the overall champion of the 6th annual Army Cyber Skills Challenge (ACSC). The event included competitors participating simultaneously from four different geographical regions throughout the U.S. and included physical, tactical, and technical challenges. (U.S. Army Photos)*

Expeditionary Cyber Operator Assessment and Selection

780th Military Intelligence Brigade (Cyber)

FORT GEORGE G. MEADE, Md. – The 780th Military Intelligence (MI) Brigade (Cyber) began hosting the Expeditionary Cyber Operator Assessment and Selection (ECOAS) process in January 2019 at Ft. Meade, Md.

The event is open to all Active Duty enlisted members and non-commissioned officers within the Military District of Washington; Fort Gordon, Ga.; Joint Base San Antonio, Texas; and Schofield Barracks, Hawaii.

The ECOAS will evaluate and select personnel through an assessment process managed by an internal panel of senior operators. An Expeditionary Cyber Operator will operate within a team construct at the battalion and company level Areas of Operation (AO). They are responsible for the direct delivery of cyber effects within the unit AO on behalf of the Department of the Army, U.S. Army Cyber Command (ARCYBER), and the 780th MI Brigade.

According to ARCYBER, Army Commanders need the ability to have freedom of maneuver in cyberspace and the electromagnetic spectrum to deliver effects in a severely contested information environment.

The Cyber Warfare Support Battalion, through the brigade combat teams, will be a tactical force for the combatant Commands to deliver effects and increase the lethality of Army commanders by developing solutions, and allowing effects to be created against tactical targets.

According to Col. Brian Vile, the commander of the 780th MI Brigade, the intent of the ECOAS process is to evaluate and select personnel to be an Expeditionary Cyber Operator.

“I want Soldiers who want to do the most challenging tactical problems in the most demanding conditions,” said Vile.

Soldiers who are interested in ECOAS should email their respective S3 (operations) section, all other inquiries will be handled by the brigade public affairs officer.

Cyber Blitz 2018 gives ARCYBER opportunity to test

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

JOINT BASE MCGUIRE-DIX-LAKEHURST, N.J. – *Cyber Blitz is informing the Army on how to employ evolving Cyber Electromagnetic Activities, or CEMA, across all aspects of the Army: doctrine, organization, training, materiel, leadership, personnel, facilities and policy, or DOTMLPF-P. This year's activities examined how the integration of Cyberspace, Electronic Warfare, Intelligence, Space, and Information Operations could help a Brigade Combat Team gain and maintain the advantage against a regional peer in multi-domain operations. (US Army COMCAM Photo)*

JOINT BASE MCGUIRE-DIX-LAKEHURST, N.J. – Soldiers and Army Civilians from U.S. Army Cyber Command (ARCYBER) and the U.S. Army Cyber Center of Excellence (CCoE) participated in Cyber Blitz 2018 (CB18) to exercise new concepts, capabilities and techniques for everything from offensive cyberspace operations (OCO) and defensive cyberspace operations (DCO), to electronic warfare (EW) and information operations (IO).

Cyber Blitz is an annual exercise co-hosted by U.S. Army Communications-Electronics Research, Development and Engineering Center (CERDEC) and the CCoE that informs the Army on how to employ cyberspace electromagnetic activities, or CEMA, across all aspects of Army doctrine, organization, training, materiel, leadership and education, personnel, facilities, and policy, or DOTMLPF-P.

"Army Cyber Command's people are in contact with adversaries every day, around the world, and constantly advancing and improving the Total Army's ability to act swiftly and decisively in cyberspace," said Brigadier General Richard E. Angle, Deputy Commanding General for Operations at U.S. Army Cyber Command. "Cyber Blitz is a tailor-made environment to put these operational lessons to the test. The integration of Information Operations, Electronic Warfare, and Cyber enables a traditional infantry brigade to quickly enter and fight within an adaptive, demanding cyber training environment. Ultimately, Cyber Blitz is elevating the entire Army's ability to train, fight, and win across all domains."

This year's activities, which took place throughout September, examined how the integration of OCO, DCO, EW, intelligence, space, and IO, could help a brigade combat team (BCT) gain and maintain the advantage against a regional peer in multi-domain operations in a no-consequence environment against live targets.

"Cyber Blitz is the only venue that allows for Army CEMA personnel across ARCYBER and FORSCOM (U.S. Army Forces Command) to be the primary training audience," said Lt. Col. Wayne Sanders, CEMA Support to Corps and Below (CSCB) chief for Army Cyber. "We can exercise new concepts, capabilities and techniques without worrying about detracting from a maneuver unit's training objectives while still being informed by expert BCT staffs and commanders who recently returned from deployment."

Sanders said ARCYBER's mission here at CB 18 was to bring the Cyber Warfare Support Battalion (CWSB) construct, which was recently approved by the U.S., Army, and the Expeditionary CEMA Team (ECT) model, that ARCYBER has been exercising at the Combat Training Centers (CTC), and exercise the full complement of the ECTs' tools and capabilities, including OCO, DCO, EW, and IO. The goal of the CSCB experiment was to provide the maneuver commander and his staff from 3rd BCT, 10th Mountain Division (3-10 MTN), with additional options within the cyberspace domain and electromagnetic spectrum to increase their lethality and create an overmatch against our near peer

new concepts, capabilities and techniques

adversaries.

"As an analyst, I'm used to the physical side – real terrain, real physical personas that we are tracking – this is more of the cyber side," said Pfc. Riley Lamas, an all source intelligence analyst with the 317th Engineer Battalion, 3-10 MTN. "We're tracking internet and cyber capabilities as a whole, (which) is totally different from what I'm used to…it's definitely unique. We've been fighting an insurgency recently and I believe the next big conflict is going to happen in cyber, so I'm taking part in something that is going to help the Army win its next battle."

The 780th Military Intelligence (MI) Brigade (Cyber), Cyber Protection Brigade (CPB), and 1st IO Command, all major subordinate commands under ARCYBER, sent Soldiers and Army Civilians to participate in the experiment to test new concepts, capabilities and techniques within their respective OCO, DCO and IO disciplines.

"Cyber Blitz is going really well. We are identifying weaknesses and patching them up – immediately, and we are finding new ways to improve our systems," said Spc. Ian Campbell, an expeditionary cyberspace operations specialist assigned to the 782nd MI Battalion (Cyber) ECT. "Additionally, we get to work with EW and the BCT staff, however, the focus is on us. It's given us the opportunity to show them what we can do and they get to see our perspective from our point of view. It's going to create a synergy between all the units and teams working together."

Maj. Nolan Barco, who is assigned to the CPB, was the DCO assessor for CB18 and he echoed the value of CB18 as a venue to test and validate new concepts and capabilities in a permissive environment. His DCO Soldiers and Civilians enhanced the BCT operations by reinforcing the tactical network and introduced the concept of securing key terrain in the electromagnetic spectrum versus geospatial.

Additionally, Soldiers representing the electronic warfare and information operations disciplines talked about the value of working with their brethren from OCO, DCO, intelligence and space.

"We're all reliant upon each other. If I'm an electronic warfare guy I'm relying on signals intelligence to tell me what my targets are. At the same time if a cyber operator needs to get to something over the radio they are going to come to me. We're all working together in one fight," said Chief Warrant Officer 2 James Gill, technical advisor to doctrine, lessons and best practices at the CCoE.

Gill served as the EW accessor for CB18 and observed how the EW, SIGINT (signals intelligence), and cyber personnel were integrating in order to take back lessons learned for the EW community.

"Cyber Blitz enables electronic warfare by allowing us to practice our tradecraft in a less constricted environment, at the same time we're the focus of the experiment," said Gill. "This gives electronic warfare personnel that focused attention just like a maneuver guy gets at the CTC so then can really practice and mold their craft."

Staff Sgt. Andrew Frame, an IO noncommissioned officer assigned to the 151st Theater Information Operations Group, U.S. Army Civil Affairs and Psychological Operations Command (USACAPOC), was at CB18 to support the ECT with intelligence.

"What excites me about my job is answering difficult questions. Doing intelligence work in both information operations and cyber," said Frame.

Continued on page 37

***JOINT BASE MCGUIRE-DIX-LAKEHURST, N.J.** – Cyber Blitz 2018 tested Cyber Electromagnetic Activities, or CEMA, concepts for the Army. (US Army COMCAM Photo)*

AvengerCon: the hacker training event for today's

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

FORT GEORGE G. MEADE, Md. – With presentations ranging from "Anatomy of a Phish" to "Sun Tzu's Art of War Applied to Cyber Operations," AvengerCon attracted more than 330 people — triple the size of just three years ago.

The hacker-style convention, hosted by the 781st Military Intelligence Battalion on Nov. 26 and 27 at McGill Training Center, was open to all service members, DoD civilians and invited guests within the information security community.

Capt. Skyler Onken, of the 781st MI Battalion, said AvengerCon is an effort from within the ranks.

"It originally came from an idea myself and [Capt. Stephen] Rogacki, had when we were attending DefCon and we saw that it was really difficult for the Army to send a lot of people to these events," he said.

"But they are really valuable in two ways. One, obviously, the educational training benefit, and two, really getting a feel for the community, because hacking and cyber are more than just a skill set or a profession. It really is a community."

Capture The Flag

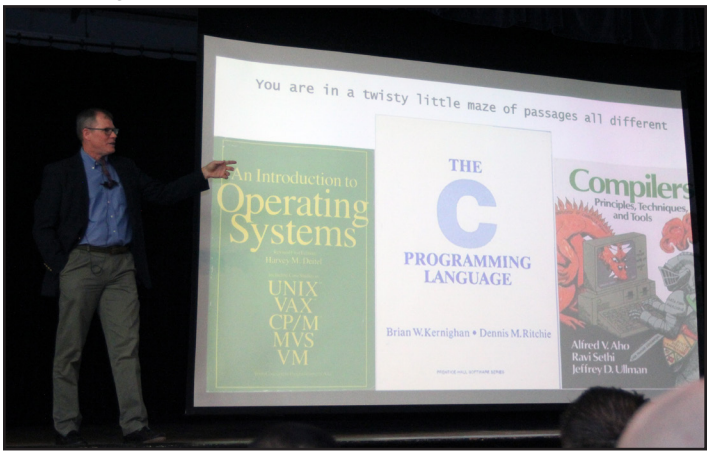
Event staff facilitated four workshops including a "fuzzing" workshop, which discovers vulnerabilities within software; a reverse engineering workshop, which has application in defensive-side power analysis and exploit development; a presentation by the Army Cyber Institute on how to create a capture-the-flag competition; and another on hacking the Internet of Things.

"This conference is great because it's a chance for the military and government-side here who aren't always allowed to go to the big conferences [and see what the community is doing]," said Grimm CEO Brian DeMuth.

Grimm, a cybersecurity engineering and consulting firm, provided organizers on the floor to interact with attendees and featured a booth that displayed the advances they've made into automotive security, among other fields.

"[Attendees] get a chance during the week to come out and hang out at this conference and learn from the people who are here," DeMuth said.

Presentations on the main stage included topics like "Integration of Open Source Web Technologies in CNO [computer network operations] Development," "Military Applications of 3-D Printing," and "An Introduction to Machine Learning, Using Machine Learning to Find the Perfect Cocktail."



FORT GEORGE G. MEADE, Md. – *Chris Eagle, a senior lecturer of Computer Science at the Naval Postgraduate School in Monterey, Calif., was the keynote speaker at the third annual AvengerCon, a hacker-style training event, at the McGill Training Center on November 27. Eagle is well known in the hacking community as well as within military circles. He has been a speaker at conferences such as Black Hat, Shmoocon, and Defcon and is the author of "The IDA Pro Book". (U.S. Army Photo)*

"My job pertains to cyber, so a lot of these talks are interesting to me, and it's just interesting to see what my other compadres are working on as well," said Interactive On-Net operator Michael Ighat of Pasadena, who works with the 780th MI.

"I like to learn more about the introductory [subjects] like the car hacking, the introduction to 3-D printing, reverse engineering — stuff like that, just to kind of broaden my spectrum. I do a lot of security, but I kind of dabble in reverse engineering. It's nice to [have this knowledge] and tools."

FORT GEORGE G. MEADE, Md. *– "Conquer the Flag" and "Howdy Neighbor IOT" (Internet of Things) capture the flag were two village events attendees could participate in at the third annual AvengerCon. (U.S. Army Photo)*

Crypto Challenge

There were plenty of booths from private organizations as well, including a crypto challenge, in which attendees could work at their own pace to solve various tasks; hacker trivia; a capture-the-flag event; lock-picking; and Grimm's supervisory control and data acquisition display.

"We as cyber security and business people tend to be interested in the interconnectivity of systems, and locks are a system that we interact with on a daily basis that very few people understand," said TOOOL Maryland Chapter president Michael Bain.

"I think it's a very good physical analog to what we face in cybersecurity. Understanding the system in its entirety is what allows you to leverage control over it."

As she worked to decrypt a new cypher, Spc. Erin Rockwell of the 780th MI said she found the lock-picking event to be especially helpful and thought the convention overall was a boon to her professional development.

"I do work with cyber, so [this conference] relates to my job," she said. "I'm learning new things that relate to my schooling."

Onken said the event is clearly continuing to grow and envisioned multiple tracks of presenters in the future to cover a broader range of topics, including possibly a classified track for cleared attendees to talk about their mission.

"I do this because I love this," Onken said. "I was hacking before I was in the Army. I joined the Army to do this, and I like to bring a lot of that passion and spirit in. [AvengerCon] will help the Soldiers to become better at what they do. I really want people to catch the bug."

Onken said he sees AvengerCon as another way the Army is aggressively pursuing cyber technology.

"From what I've seen — and I've worked with all the other branches — the Army is absolutely the most aggressive in pursuing advancements in the way that we manage people, the way we manage mission," he said.

"For being a larger organization we've actually done really well at being adaptable to the environment. In this environment, you always need to be more adaptable. But right now, the Army is definitely ahead of their peers."

Editor's note: Soundoff Staff Writer Jack Chavez contributed to this article.

Capt. Onken wants to recognize Sgt. 1st Class Craig Seiler as one of the AvengerCon originators, and thank the Cyber Solutions Detachment and C Co., 781st MI Bn., who were key in this year's planning and execution.

FORT GEORGE G. MEADE, Md. *– One of the village events at this year's AvengerCon III included a lock pick village put on by TOOOL (The Open Organisation of Lockpickers), a local locksport, lock-picking organization. (U.S. Army Photo)*

The Maginot Line: Fulfilling the Army Cyber Vision through

By 2nd Lt. Joseph Kim, A Company, 781st Military Intelligence Battalion (Cyber)

The vision for cyber in the Army can essentially be boiled down to being an innovative cyberspace operations force that can design, build, and deliver integrated capabilities in order to deter and defeat our enemies. While there remain many questions on how to best fulfill this vision, we can learn lessons from the successes and mistakes of those that have come before us, even before the dawn of "cyber warfare." One such event which provides great insight into the innovation and integration of new technologies into multiple domains of battle is the German campaign against the French that overcame the great defensive barrier that was The Maginot Line.

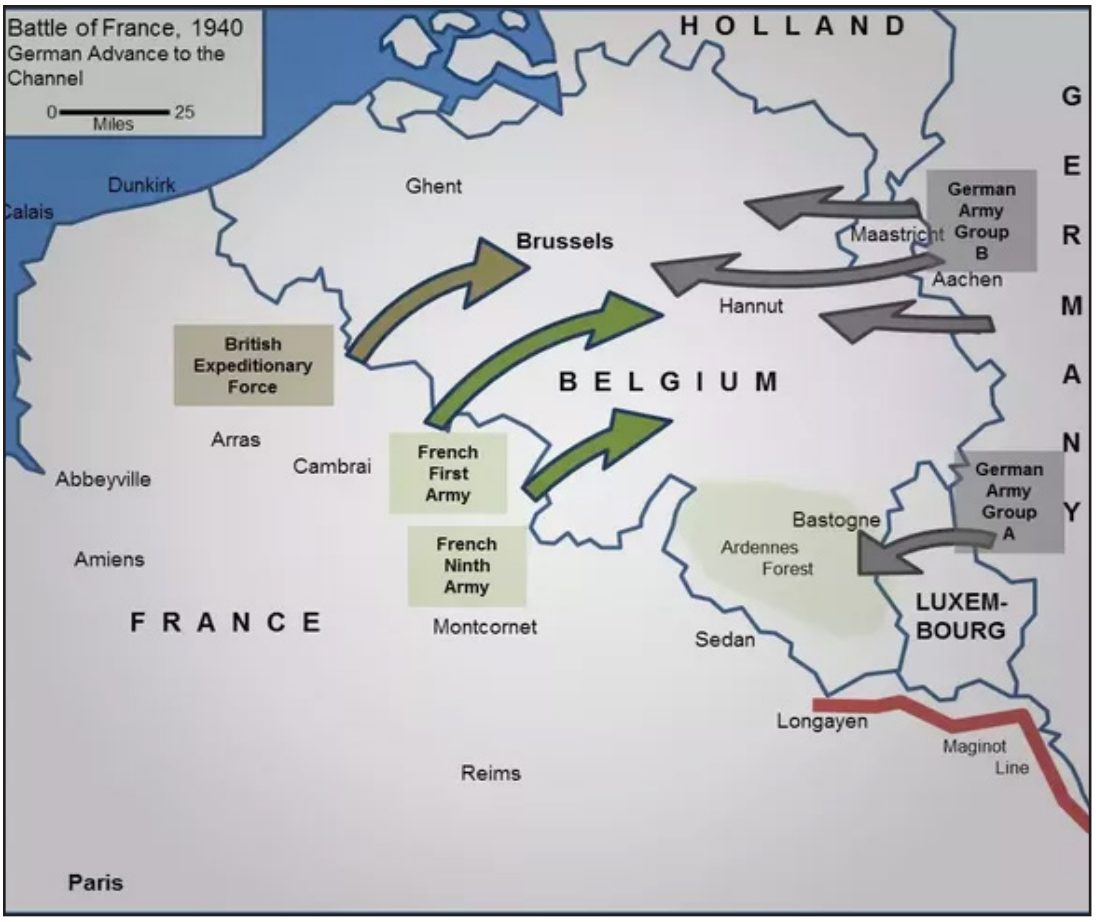
In the aftermath of World War I (WWI), France constructed the Maginot Line in order to prevent the death and destruction that had occurred as a result of the static trench warfare prevalent during that conflict. The Maginot Line was a very extraordinary defensive military achievement built to deter the enemies of the French and help them to defeat their adversaries, specifically, the Germans, if they attempted to attack using the tactics and techniques seen in WWI. However, the Maginot Line had two major failings. It did not consist of mobile defensive pieces and it relied on the Ardennes region as a part of its fortification. The French assumed that the Ardennes – a region of extensive forests, rough terrain, rolling hills and ridges – would be impenetrable. In fact, they did not even extend the line all the way to the English Channel. If an enemy found a way to exploit the weakness on the line in the Ardennes region they would be able to cross into France and successfully invade the country, making the rest of the Maginot Line relatively pointless.

In May of 1940, the Germans did just this. They adapted to the new situation at hand and utilized the doctrine of Blitzkrieg. The speed with which Germany was able to attack France and then get through the Ardennes successfully isolated all the forts on the Line. The Germans attacked through Ardennes, which was believed to be impassable by the French. The lack of mobility due to the Line being made up of a series of forts rather than mobile units caused the French soldiers to remain isolated upon the German invasion and allowed the Germans to attack the Line from behind. While the Maginot Line was built to be tough against tanks and infantry, it did not consider the ability of the enemy to take advantage of multiple domains of battle. Nazi Germany was able to exploit the advantages they had in air superiority as well in order to launch massive air attacks and completely fly over the Line with little consequence. This successful implementation of Blitzkrieg demonstrated the importance of adaptation and extending the battlefield over multiple domains.

German engineers clear a barricade of trees in the Ardennes Forest to allow the panzers to pass.

rapid adaptation and Multi-Domain integration

The Germans' ability to adapt to their situation at hand and combine maneuver across multiple domains essentially rendered the French helpless and led to the successful invasion of France. Just as the Germans exploited the technology of tanks and airplanes to gain advantage over the French and British forces, commanders must do the same today in order to achieve the Army Cyber vision of being 'a force that designs, builds, and delivers integrated capabilities'. Commanders must be able to help develop new cyberspace capabilities and encourage innovation throughout the process



This map of the Battle of France, 1940 shows the approximate positions of the British Expeditionary Force, and the French First and Ninth Army as they lined up against the German Army Group A and Group B. Note where the Maginot Line ends.

of integrating within the multiple domains. The Germans were able to take the innovations in their technologies and rapidly apply them to the battlefield's various domains. We must be able to do the same with our capabilities and incorporate them quickly in order to address the dynamic battle space that is cyber.

While we can learn from Germany's success, the French have valuable lessons that we can learn from as well. They built the Maginot Line in order to avoid the disaster that befell them during World War I. However, they built this great defensive monument with a limited view of the battlefield and only visualized a stagnant, non-evolving form of war. Commanders in the cyber realm must seek to visualize the entire battlefield as dynamic and ever-changing, especially in order to avoid the potential conflicts between each of the domains as well as between organizations. Finally, as peer adversaries continue to develop their cyber warfare capabilities, we must not remain content with our capabilities, as the French did with their Maginot Line, but continue to adapt and integrate ourselves in multi-domain conflict in order to provide the greater Army with the ability to 'win decisively against any adversary, anytime and anywhere, in a joint, multi-domain, high-intensity conflict'.

Should Cyber be fun?
"Extracurricular Cyber" Helps Achieve the Cyber Vision

By 2nd Lt. Orion Williams, C Company, 781st Military Intelligence Battalion (Cyber)

Over the past few months I have been lucky enough to participate in two unique and exciting training opportunities that had almost nothing to do with my day job: the Tatooine Bug-Bounty in Augusta, Ga., and the Army Cyber Skills Challenge (ACSC) at the Ft. Meade, Md. Neither event trained me directly for any scenario that I would experience on a Cyber team, yet I can confidently say I have gained valuable experiences from both that will shape my future career. On a grander scale, I would argue events such as these, though perhaps trivial or superfluous at first glance, are key to the Cyber branch's achievement of its overall Cyber Vision. While it would be ludicrous to argue that these events resemble a typical Cyber day job, they benefit the Army Cyber community by inviting newcomers into the subject matter, turning learning and networking into a game, and – perhaps most significantly – fostering a closer knit Cyber community and better overall branch culture.

The Army Cyber vision states: "U.S. Army Cyber Command integrates and conducts full-spectrum cyberspace operations, electronic warfare, and information operations, ensuring freedom of action for friendly forces in and through the cyber domain and information environment, while denying the same to our adversaries." This practical, militaristic mission statement appears to leave little room for fun. Recreational hackathons and internal competitions would just take time, energy, and manpower away from 'the real stuff.' In reality, such an assessment denies the intangible, long-term benefits of these events. For one, these events invite new, diverse talent into the Cyber realm. Because these events are accessible to all skill levels, they provide a safe environment for Soldiers to foster their interests in a wide variety of computing categories. By creating an environment predicated on fun and focusing on self-paced activities, the uninitiated can delve into topics that once seemed unconquerable.

Furthermore, these benefits are not restricted to novices: recreational Cyber events also promote continued learning and networking throughout the branch. Though framed as individual challenges, nearly all of these events have a mentorship component to help guide participants. For example, Warrant Officers were always available to help participants work through difficult portions of the ACSC. Soldiers were able to learn directly from subject matter experts while also meeting new individuals with whom they may otherwise never have interacted. The competitive nature of these events keeps everyone motivated and engaged.

Finally, these events foster the overall culture and community of the Cyber branch. Perhaps due to its recent inception, Army Cyber can sometimes feel like an incoherent community. All of its senior leaders spent their early careers in other branches, bringing bits and pieces of those cultures with them. By encouraging participation in community-based, recreational Cyber events, the branch can construct its own identity and culture. Through informal mentorship and social engagement at these events, participants are unwittingly building the Army Cyber community of the future. Unspoken bonds and common ideals are indispensible in the creation of a hard-working, focused force. Recreational Cyber events provide an ideal setting for both the maintenance of old bonds and the induction of new members into the fold.

Though counterintuitive at first glance, fun events and gatherings such as the Tatooine Hackathon and the ACSC are requisite for the realization of the Army Cyber Vision. Not only do these events increase the skill base of Army Cyber soldiers, but they also build a shared Cyber culture, uniting this small branch as it advances into the future. As commanders encourage their soldiers to participate in these events, they are actively building the improved Cyber force of tomorrow.

DDS Bug Bounty

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

***AUGUSTA, Ga.** – Soldiers from the 780th Military Intelligence (MI) Brigade (Cyber) joined fellow Army Soldiers and Civilians, industry partners and academia in a live bug bounty event hosted by the Defense Digital Service (DDS) at the new Georgia Cyber Center October 25. (U.S. Army Photo)*

AUGUSTA, Ga. – Soldiers from the 780th Military Intelligence (MI) Brigade (Cyber) joined fellow Army Soldiers and Civilians, industry partners and academia in a live bug bounty event hosted by the Defense Digital Service (DDS) at the new Georgia Cyber Center October 25.

DDS hosted the live bug bounty event to allow Soldiers and other participants to showcase their talents and develop new skills.

The event operated under the DoD Vulnerability Disclosure Program's rules. DDS invited hackers of all skill levels to participate and there were HackerOne personnel, a DDS vendor, present for some over-the-shoulder coaching.

The event included an open house and tech showcase, including a speaker series with Chris Lynch, director of the Defense Digital Service, senior U.S. Army Cyber Command (ARCYBER) leadership, Milo Medin, vice president at Google and Defense Innovation Board member, and a panel of DDS and military participants in the Jyn Erso (JYN) program.

"It was a fun event, and the number one bounty found for the day was found by an AIT (advanced individual training) private," said Army Capt. Alexander Master, commander, B Company, 781st MI Battalion (Cyber). "He managed to access an Army helpdesk webpage without authentication, then dumped the PII information for all service members who had ever submitted tickets into the system, and demonstrate how he did it to all in attendance."

DDS hosted the inaugural event to mark the fact that they have leased out office space, which they are calling Tatooine (Star Wars reference), in the new Georgia Cyber Center in downtown Augusta.

According to Brig. Gen. Joseph Hartman, deputy commanding general, Joint Force Headquarters – ARCYBER, "the space will be used to support several partnerships between DDS, ARCYBER, and the CCoE (Cyber Center of Excellence), to include our JYN program and the Advanced Education Program (AEP) to build Army Tool Developers."

The event included participants from the 780th MI Brigade, headquartered at Fort Meade, Md., with battalions at Meade and Fort Gordon, Ga.; the Cyber Protection Brigade and CCoE, both based at Ft. Gordon; and Augusta University students. The bug bounty allowed hackers, service members, industry partners and academia to hack *.army.mil/* webpages.

"(It was a) great experience, and we look forward to doing more bug bounty programs through HackerOne to find and hopefully assist DODIN (Department of Defense Information Network) in identifying and remediating web vulnerabilities," said Master.

Placing overall in the bug bounty event and representing the 781st MI Battalion were 1st Lt. William Brattain, who placed second, and Maj. Colin Kinsella, who placed third.

November 30th, 2018
Marriott BWI Airport

BALTIMORE – Soldiers, Army Civilians, contractors and their Family members of the 780th Military Intelligence (MI) Brigade (Cyber) started the festive season by getting together for a formal occasion at their annual Holiday Ball at the Marriott BWI Airport hotel on Nov. 30.

The receiving line for the Holiday Ball included the keynote speaker, Maj. Gen. George Franz, managing director AFS and former director of operations for U.S. Cyber Command, the brigade commander, Col. Brian Vile, and the brigade senior enlisted advisor, Command Sgt. Maj. James Krog, and their spouses.

Guests were welcomed to the Holiday Ball by the receiving line.

The Holiday Ball included Soldiers and Army Civilians, accompanied by their spouses, friends, and Family.

The Holiday Ball included Soldiers and Army Civilians, accompanied by their spouses, friends, and Family.

The Holiday Ball began with the posting of the Colors, an invocation and a stirring rendition of our National Anthem presented by the USO Show Troupe.

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

The USO Show Troupe stayed throughout the event to provide Holiday cheer.

The keynote speaker, Maj. Gen. George Franz, managing director AFS and former director of operations for U.S. Cyber Command,

There was a cake cutting to recognize the youngest and oldest members of the Brigade.

After the retiring of the Colors, the evening ended with dancing.

2018 Holiday Ball Honorees

The Honorable Order of Saint Isidore is awarded to those individuals who have demonstrated the highest standards of honor and moral character, and provided considerable and lasting contributions to the U.S. Army Cyber Command. Their character, values and warrior ethos epitomize the cyber warrior spirit and they live by the Command's motto, "Second to None."

Maj. Jason Seales was a Silver Award inductee into the Honorable Order of Saint Isidore.

Mrs. Connie Hamilton was a Bronze Award inductee into the Honorable Order of Saint Isidore.

The 780th Military Intelligence Brigade (Cyber) Soldier of the Year is Spc. Alexander Musarra, and the NCO of the Year is Staff Sgt. Savannah Matelski.

The 780th Military Intelligence Brigade (Cyber) Linguist of the Year is Spc. Alexander Musarra.

The Army Cyber Vision

By Spc. Stephen Nicholas, 01 N-CPT, D Company, 781st Military Intelligence Battalion (Cyber)

The U.S. Army's Vision states, "The Army of 2028 will be ready to deploy, fight, and win decisively against any adversary, anytime and anywhere, in a joint, multi-domain, high-intensity conflict, while simultaneously deterring others and maintaining its ability to conduct irregular warfare…" ARCYBER (U.S. Army Cyber Command) further augments this by stating its vision of aggressively operating and defending our networks, data, and weapons systems.

While I cannot delve too deeply into how exactly we support this, I can explain the theoretical concepts and practices we follow. Being a National Cyber Protection Team, our mission is to rapidly evaluate, and act in response to unexpected and dynamic cyber situations. We defend the nation in response to hostile and imminent cyber threats. This includes global operations to deter, disrupt, and defeat our adversary's cyberspace operations to ensure that the United States has the freedom to maneuver within our global infrastructure and ensure that Commanders across the world can carry out their missions. With this, we wholeheartedly support the Army's vision to conduct irregular warfare.

Attacks on our networks are ever constant and an adversary only needs to be successful once while defenders need to be successful every time. With this approach, we hone our TTPs (tactics, techniques, and procedures) and tradecraft to both harden our perimeters and rapidly respond to compromises within. Our combatant commands rely on secure communications, the integrity of their data, and the availability of their systems. Our nation's infrastructure (i.e. energy, financial, etc.) provides the foundation for our daily lives. If these systems were not secure and responded to, our national interests and way of life would be severely degraded. By constantly improving upon our technical knowledge, utilizing and expanding upon our toolsets, and creating partnerships, we can aggressively support the visions of the U.S. Army and ARCYBER.

An essential piece of defense is to utilize the Defense-in-Depth framework. By using this, organizations can reduce the success of threats and minimize the damage done when our adversaries succeed in penetrating our defenses. The hardest element of defense is responding to zero-day attacks. Exploits in coding never seen before in "the wild" can be resource-intensive in identifying and developing methods to patch the weaknesses these attacks utilize. By constantly training, reading publications, and working with other entities in the cyber field, we ensure that ARCYBER's vision to ensure the integrity of our infrastructure, regardless of the system or location.

Finally, the concept of cyber is irregular in of itself. The United States Army called for the development of a force that can be highly flexible and maintain our organization's ability to conduct global operations. We, cyber, answered that call. We do not need to be at the enemy's doorstep. While we are all Soldiers at the core, our primary weapon system is not the M4 Carbine. Our primary system is the computer. Straying from the stereotypical kinetic options has enabled us to carry out our mission set in unconventional ways, many of which our adversaries did not foresee being operational in such a short span of time.

***BALTIMORE** -- Sgt. Lord Larsen and Sgt. Juan Melendez, both assigned to D Company, 781st Military Intelligence (MI) Battalion (Cyber), reenlisted in the U.S. Army in front of friends, Family, and fellow Soldiers at the Federal Hill Park on Oct. 26. (U.S. Army photo)*

Volunteering can impact our future leaders

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

***ODENTON, Md.** – Staff Sgt. Sosi Alexanian and Spc. Kayla Lee, both from C Company, 781st Military Intelligence Battalion, were at Nichols-Bethel United Methodist Church to teach the girls of Girl Scout Junior Troop 1398 about U.S. flag etiquette. (Courtesy Photo)*

ODENTON, Md. -- Staff Sgt. Sosi Alexanian and Spc. Kayla Lee, both from C Company, 781st Military Intelligence (MI) Battalion (Cyber), were at Nichols-Bethel United Methodist Church to teach the girls of Girl Scout Junior Troop 1398 about U.S. flag etiquette and being part of a Color Guard.

Troop 1398 is hoping to be selected to do the flag ceremony at a Bridging Ceremony which is when a Girl Scout rises to the next level - in their case moving up from Juniors to Cadettes. According to the Troop's leader many of the girls have a parent or family member in the military so this was a great way to honor them.

About two weeks before the event, a fellow Soldier on the 781st MI Battalion funeral detail team saw a post on a community Facebook page requesting local military members to teach flag etiquette and color guard procedures to Girl Scout Troop 1398.

Alexanian and Lee volunteered to help. Their service was not required and no one outside of the funeral detail team knew about it. At the end of the evening the Soldiers took a group photo for the Troop to keep.

"I volunteered because I saw an opportunity to work with kids in our community that I wouldn't normally get to interact with," said Lee. "I love to teach and share the knowledge I've gained in the Army, in this case, my knowledge of flag etiquette I learned from being on the Battalion Funeral Detail team. I saw this as an opportunity to help the community while doing something that I enjoy."

Lee hopes the Troop reaches out to them in the future and believes it's important for the military to maintain relationships with different organizations in their local communities.

"This volunteer event is important to me because I got to impact a group of young girls who will continue to grow and turn into leaders. It was especially important to me to volunteer to work with these girls because I want to be a role model for them," said Lee. "I wanted to share that it doesn't matter what size or gender someone is as long as you are passionate about what you want to do."

Overcoming the Battle of Tomorrow, Today.

By Capt. Kyle Yoder and Capt. Ian Howard, Detachment Texas, 782nd Military Intelligence Battalion (Cyber)

As cyberspace operations increase in complexity and frequency around the world, training of future Soldiers, Sailors, Airmen, and Marines will become a priority for the nation. A high operations tempo mixed with a necessity for trained and motivated personnel will continue to be a bottleneck for units and their real-world operations.

U.S. Cyber Command's emphasis on assigning highly trained personnel to units will keep the ranks of the cyber force filled. However, for these newly trained cyber warriors to be ready to start their career in this evolving field -- it will be through the mentorship of experienced NCOs and petty officers across all services that we develop a thriving cyber force for tomorrow.

Moving forward, we look to the U.S. Army Cyber Command (ARCYBER) Vision for a source of continual progression on what the Army and nation will need in the years to come as well as shaping the newest members of the force:

> *"A force that can aggressively operate and defend our networks, data, and weapons systems; A force which delivers effects against our adversaries in and through cyberspace to enable commander's objectives; A force that designs, builds, and delivers integrated capabilities for the future fight – spanning cyberspace, electronic warfare, and information operations. We do this by developing our people, improving our processes, and building partnerships."*

Breaking down the guidance offered by ARCYBER, the last line offers both a goal and a challenge to the leaders of the cyber force that can directly benefit both new and senior Soldiers alike. The training we receive will prepare us to deliver effects today; however, it is the adversary of tomorrow we should be preparing to face.

Soldier development remains a core tenant of any NCO in the Army. With the evolving battlefield we face today, this task only increases in difficulty. The "development of our people" is not a new concept to Army leadership, but will offer new challenges as we develop training plans due to the relatively young age of the Cyber Branch. As the youngest branch in the Army, the Cyber Corps is still developing traditions and legacies at a much earlier state than other branches.

The cyber warfighter faces new difficulties in "improving our processes". The Army constantly adapts to the fight before it, but in cyberspace, often, these changes occur at a faster rate than our basic training can keep up with. Leaders in the cyber force face the task of creating new training plans while adapting to old systems in order to handle new challenges. The ability to rapidly shift focus and overcome these ever-changing requirements will speak to the strength and future development of the Cyber Corps.

Finally, "building partnerships," is not a new concept to the armed services, but in current cyberspace operations more and more frequently Soldiers will find themselves working among Sailors and Airmen. This will not result in undue strife within the ranks, but responsibilities inherited here will demand that leaders adapt their way of joint mission development. Similar to our own Soldiers, they will constantly need mentorship in the shifting landscape of the cyber battlefield. Officers, Warrant Officers, and NCOs in the Army will need to ensure the Sailors and Airmen assigned to their unit receive the mentorship and training needed to advance their own knowledge and careers.

The idea of training Soldiers, adapting to change, and working with other services is not a task that should intimidate our leaders. However, we need to remain proactive as the scope and complexity of cyber operations is constantly shifting and growing; being ready to handle these changes now is what will set us apart. In order to always be in the fight we must predict and overcome the battle of tomorrow, today.

Army National Guard cyber Soldiers update their

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

***FORT GEORGE G. MEADE, Md.** – Lt. Gen. Stephen Fogarty, commanding general, U.S. Army Cyber Command, talks to distinguished visitors from the National Guard thanking them for their support of Task Force Echo and providing them with an update on the state of the command at the 780th Military Intelligence Brigade (Cyber) headquarters on November 3. (U.S. Army Photo)*

FORT GEORGE G. MEADE, Md. – Army National Guard Soldiers (ARNG) assigned to Task Force Echo hosted distinguished visitors (DVs) from their home states in order to update them on the Cyber Enterprise and their operations in support of U.S. Army Cyber Command (ARCYBER) and U.S. Cyber Command (USCYBERCOM) at the 780th Military Intelligence (MI) Brigade (Cyber) headquarters, November 2 and 3.

Task Force Echo consists of more 130 ARNG Soldiers, primarily assigned to the 125th Cyber Protection Battalion (CPB), who hail from Louisiana, Mississippi, New Jersey, New York, South Carolina, Texas and Utah. The Task Force is commanded by Lt. Col. Linda Riedel with Command Sgt. Maj. William Kyzer as the senior enlisted leader. Riedel is the first commander of the 125th CPB and prepared the formation for deployment in support of Task Force Echo in March 2018.

Since April, this second iteration of Task Force Echo – aligned under the active Army's 780th MI Brigade – has been conducting technical training and supporting ARCYBER and USCYBERCOM missions.

Riedel, who hails from South Carolina, hosted the event in order to inform the National Guard leadership of the critical importance of the Task Force Echo mission to USCYBERCOM and the Cyber National Mission Force, as well as the return investment for the states and the nation.

"The intent is to bring the state leadership together so they can observe what their Soldiers are doing on mission in support of U.S. Cyber Command and Army Cyber," said Riedel. "I want them to be able to meet and cross talk with other cyber leaders and have the conversations at the table. It's important that we sustain and maintain the training and expertise of our Soldiers. Building those relationships across the states is vital to our success. As (Lt. Gen.) General (Stephen) Fogarty mentioned (the commanding general for ARCYBER), 'we are writing the book.'"

In recognition of the critical role the National Guard has in support of the ARCYBER and USCYBERCOM mission, Lt. Gen. Fogarty thanked the DVs for supporting Task Force Echo and remarked that this specific active and Guard partnership would continue for the foreseeable future. He also talked about how the Army was working with the other Services and the way ahead which ultimately benefits the states, the Army and the nation.

When asked what the primary take-away for the event was, Riedel said "their Cyber Warriors are

State leaders

value added not only to the (Task Force Echo) mission but to their states. Cyber Training is expensive and must have the full buy-in of all leaders."

"I want the DVs to leave with a firm understanding of what the National Guard cyber warriors bring to the fight and how dedicated our cyber warriors are to the success of this mission," added Kyzer.

The first briefing the DVs received was an Executive Cyberspace Operations Seminar presented by the Cyber Center of Excellence. ECOS familiarizes general officers, senior executives, and senior commanders with cyberspace operations, and policy considerations; threat characteristics; lessons learned from recent and ongoing cyberspace operations; and ARCYBER's strategy and vision.

"Title 32 (federal authority over National Guard members) we know allows certain authorizations, Title 10 (federal authority over Service members), and so forth. I learned there are more Titles than I realized and that we can do a lot more if we are actually on that Title," said Col. John Nip, G6 (signal), Joint Force Headquarters, Mississippi ARNG. "That allows us to support the state better and the nation, because ultimately that state mission, our domestic operations, are fully trying to engage the cyber protection teams in all of our domestic operations. Also, if there is a real world scenario, that we can bring a capability and capacity to the state, but also still support the Federal mission."

Nip explained it has only been 18 months since the states received the authorization to stand up the ARNG Cyber Protection Teams (CPTs). However, as a result of the Task Force Echo mission, the ARNG cyber Soldiers from Louisiana, Texas and Mississippi are "light years ahead of where they would be in a normal progression through the system as a Guardsmen."

"(Task Force Echo) has allowed us to send our Soldiers to come up here and actually get certified and get the education and experience they need to get to the CPTs to IOC (initial operating capacity) and FOC (fully operational capacity)," said Nip. "When they come back they will bring so much skill set with so much experience…and get us to the point where we can start providing those missions to the state like my Adjutant General wants us to do."

Nip said he fully supports opportunities such as Task Force Echo, whether it's a three-year or four-year rotation, because it is important to keep the skill sets viable for the ARNG cyber Soldiers and the return investment is worth the time these Soldiers spend away from their respective states.

Continued on page 37

FORT GEORGE G. MEADE, Md. *– Army National Guard Soldiers assigned to Task Force Echo hosted distinguished visitors from their home states in order to update them on the Cyber Enterprise and their operations in support of U.S. Cyber Command and the Cyber National Mission Force at the 780th Military Intelligence (MI) Brigade (Cyber) headquarters, November 2 and 3. (U.S. Army Photo)*

Task Force Echo hosts NCO Induction ceremony -

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

FORT GEORGE G. MEADE, Md. *– Army National Guard Soldiers assigned to Task Force Echo recite the Noncommissioned Officer (NCO) Creed at an NCO Induction Ceremony at the Post Theater, Sept. 18. (U.S. Army Photo)*

FORT GEORGE G. MEADE, Md. – Seven Army National Guard (ARNG) Soldiers were welcomed into the Army's noncommissioned officer ranks in a ceremony at the post theater here, Sept. 18.

Task Force Echo, an ARNG cyberspace operations formation, hosted the Noncommissioned Officer (NCO) Induction Ceremony, an event steeped in tradition during which the new NCOs were inducted into the Army NCO Corps. Two of the participants were promoted to sergeant during the ceremony.

The newly inducted NCOs are: Sgt. Jessica Atkinson, Cyber Protection Team (CPT) 173, N.Y. ARNG; Sgt. Chrisshawna Byers, 125th Cyber Protection Battalion (CPB), S.C. ARNG; Sgt. Roderick Gaskins, 125th CPB, S.C. ARNG; Sgt. Todd Marino, CPT 173, N.J. ARNG; Sgt. Michael McNamee, 125th CPB, S.C. ARNG; Sgt. Antwan Reed, 125th CPB, S.C. ARNG; and Sgt. Christopher Reyes, CPT 173, N.J. ARNG.

Guest speaker Sgt. Maj. of the Army (Ret.) Kenneth O. Preston, who served as the 13th Sergeant Major of the Army (SMA) had advice for the newly inducted NCOs and the event's audience. Speaking first to the inductees, he told the story of a private first class who asked him what he had to do to become the Sergeant Major of the Army.

"To get promoted, to be successful in your occupational specialty, to move up through the ranks to take on positions of increased responsibility: first thing, you've got to be a good Soldier," said Preston. "Be on time for formations, be in the right uniform, be STRAC (strictly according to regulations and policies); also be respectful, treat people with decency and respect, treat them as you'd want to be treated. And the last thing I told him was: be a subject-matter expert... excellence in your profession"

"And then as you become an expert, when it comes time to be a noncommissioned officer, it becomes very easy, because at that point you really become a teacher, and what you want to do is take that piece of the Army that you've been entrusted with, those two or three Soldiers, and take everything that you've learned on this journey and teach your Soldiers to be as good as you were," advised Preston.

His parting words were a challenge for the more senior NCOs and leaders in the theater.

"It was interesting. In this morning's (Association of the United States Army) newsletter there was a quote that I'd written a number of years back. … The quote says, 'The solution for many of the challenges leaders face in their units today is the simple sharing of knowledge and experience'", said Preston. "Teach your junior NCOs what right looks like. So I share that with everyone here in the audience because we now take on the responsibility for this new group of noncommissioned officers that are stepping forward to be the future leaders of our Army."

Reyes, who hails from New York City, New Jersey ARNG, was one of the two sergeants promoted during the ceremony. He said his new role is "… no longer about getting the job done at a lower level. It's making sure you are good to go as well as the Soldiers around you."

- SMA Preston keynote speaker

Reyes said his role as an Army cyber professional is fulfilling both his military and civilian goals.

"My goal is to stay in the National Guard and do good things not only for the state but also the country," said Reyes. "I also want to leverage that with my civilian career, as cyber is the new up-and-coming hot thing right now."

As the 13th Sergeant Major of the Army stated in his remarks, Reyes will not embark on his journey alone. Each of the newly inducted NCOs can lean on each other, as well as the other senior NCOs in the Task Force, as well as throughout the Army.

Task Force Echo consists of ARNG Soldiers assigned to the 125th Cyber Protection Battalion (CPB) who hail from Louisiana, Mississippi, New Jersey, New York, South Carolina, Texas and Utah. The Task Force is commanded by Lt. Col. Linda Riedel with Command Sgt. Maj. William Kyzer as the command sergeant major. Since April, the task force is aligned under the active Army's 780th Military Intelligence Brigade, and has been conducting cyberspace operations in support of U.S. Cyber Command and the Cyber National Mission Force.

FORT GEORGE G. MEADE, Md. *– Task Force Echo, an Army National Guard (ARNG) cyberspace operations formation, hosted a Noncommissioned Officer Induction Ceremony at the Post Theater, Sept. 18, and the guest speaker was retired Sgt. Maj. of the Army Kenneth O. Preston, the 13th Sergeant Major of the Army. (U.S. Army Photo)*

Dignity and Respect

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

Anyone who has been through SHARP (Sexual Harassment/Assault Response and Prevention) training or has listened to any of the #MeToo movement has heard the statistics; one in six men and one in four women have been sexually assaulted sometime in their lifetime. Those figures run the gamut from a non-consensual touch over clothing to a violent rape, either by a stranger or someone known to the victim (75 percent of the time, the subject is known to the victim) and everything in between. These statistics also include marital rape and child sexual abuse.

Personally, I have had a very hard time processing some recent political events, specifically the media coverage surrounding the confirmation of Associate Justice Brett Kavanaugh. Notwithstanding whether you agreed with the confirmation or not, it has brought to light several issues regarding sexual assault and how divided our country is about believing victims of sexual assault and many of the rape myths that have been perpetuated throughout history. This confirmation process, and the media surrounding it, has been extremely tough for many survivors of sexual assault. The media, various politicians, and most of the general public do not understand the neurobiology and psychology of trauma after a sexual assault.

By no means do I ever claim to be an expert, but I do understand and empathize with survivors. Every single victim will act differently. This is one of the misconceptions, or rape myths, out there. Victims may be angry, scared, or even laugh as their coping mechanism to deal with the trauma. They may feel guilty. Many feel it was somehow their fault (it wasn't!). Some even want to protect the perpetrator (They have a family…). There is no cookie cutter response to sexual trauma.

I can't tell you how many times I have heard someone say "if that ever happened to me, I'd fight back." Our brains do not work that way. The brain takes over during trauma and puts us into a survival mode. It may mean fight, flight, or freeze; it may mean completely shutting your body down. For example, I was in a very bad car accident about 20 years ago. I did not hit my head, however I was momentarily unconscious. I saw the accident coming and my body shut down so I could survive the trauma (and thanks to my seat belt, I am here today). Unless we train and train and train ourselves on how to react, so the act becomes second nature, we don't know how we will react until we are actually in that situation.

Another rape myth revolves around reporting, or delayed reporting. Victims and survivors will report on their own timeline – or may never report – or may share their story decades later. Just because they don't report right away doesn't mean it didn't happen. Sometimes they just need time to process and accept what happened.

When someone hears the sexual assault story of another, the receiver is being trusted with one of the most personal stories the survivor has ever told. Imagine sharing this deep, personal secret and not being believed. Then having to tell it again and again through a reporting process, and not being believed or at least people being skeptical of your story. Then, if it comes to trial, the defense trying to make the situation to be a misunderstanding, portray the survivor to be promiscuous or worse, a liar. And then we, the public, the media, etc., wonder why victims don't come forward to report? Furthermore, when a survivor hears that another survivor's report is questioned, survivors understand it as they, too, won't be believed as well.

Listening and believing are ways of treating others with dignity and respect. Our words have so much power. We can build up or tear down someone with just our words. Our words may not be directed to a specific person, but when overheard can be taken to heart. We don't know who the survivors are in our units. They may be the coworker with whom you share a cubicle. We can all use a little reminder to watch what we say and ensure we are always coming from a place of dignity and respect.

U.S. ARMY

I.A.M. STRONG™
INTERVENE ★ ACT ★ MOTIVATE

The Army EO Program and Cyber

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

The Army's Equal Opportunity (EO) program is not for any one specific MOS (military occupational specialty) or command. It is something that applies to every individual unit, down to the individual Soldier or Civilian, and their families. The Army Cyber vision is "A force that can aggressively operate and defend our networks, data, and weapon systems." If one or more persons is being discriminated against, then they cannot possibly be relied on to meet this vision through their mission contributions. As with any issue, if it consumes a person's thoughts and behaviors, they will not be able to focus on their mission. Unit personnel who feel discriminated against will have to take time away from mission to file complaints, speak with commanders or investigating officers, and be away for other reasons related to the complaint. In addition, others who are called as witnesses will be required to do the same. Soon you have an entire section or workgroup involved in something that may have originally been said as "just a joke," or as "that's how it is here."

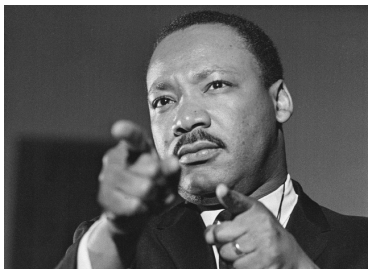
Missions in the realm of Cyber are fast-paced, and if unit personnel with specific skillsets are not present at a vital time, it could mean complete mission failure. It is imperative that all personnel are ready and able, both physically and mentally, to conduct their mission on a daily basis. There is no place in the unit or the Army for discrimination, and all personnel who feel they are being discriminated against have a right to file a complaint without fear from reprisal.

The EO program handles complaints for six protected categories: race, color, religion, sex (gender and transgender), national origin, and sexual orientation. An individual's perception determines if an incident is complaint worthy, regardless of the intent of the person committing the offense. It is important to keep this in mind and to also keep in mind how others may perceive your words and behaviors.

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 to choose from. Most museums are free or cost very little to visit, and are a great way to experience and learn about other cultures at your own pace. Learning about other cultures is a great way to gain an understanding of why people who are different may behave a certain way in specific 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.

- Martin Luther King Jr. Birthday Celebration – January 21, 2019



- National African American / Black History Month – February 2019
- Women's History Month – March 2019

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.

Word of the Day: Friend

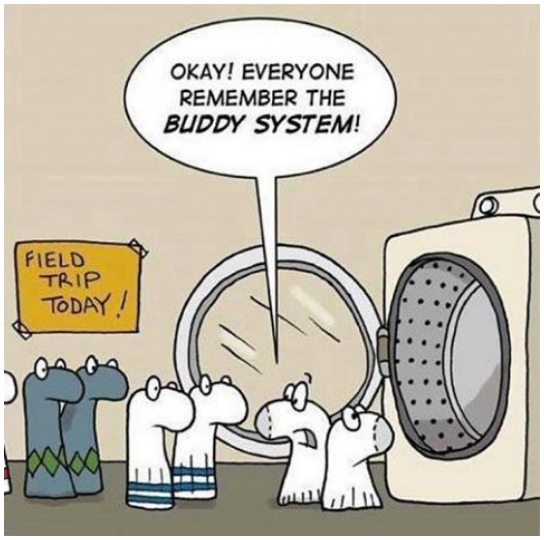
By CH (Capt.) Mike Cerula, 781st Military Intelligence Battalion Chaplain

Someday I would like to teach a class to my Soldiers and Civilians. I'd call it Friendship 101.

The more I meet and greet Cyber Warriors I realize we have a smart, motivated, hard-working group, ready to pour their all into the mission (when allowed and not busy with pipeline training); but ask them how many close friends they have and you sometimes see them raise their hand to show you the number… it's zero… zippo!

I would encourage some of these men and women to sit with other people at lunch. Their first question can be simple, 'hey can I sit with you?' Then, follow up with, 'where are you from?' or 'what do you like to do for fun?' That might be all you discuss that day, but it's a start!

The importance of having real friends and not just online acquaintances cannot be overstated. Of course it won't happen overnight, practically nothing worthwhile happens fast. Building relationships over the course of years, ensures that if today was the worst day of my life, I would be able to call my close two, three, or four friends and be certain, that they would stop what they're doing and talk to me. I would have the foundation of months or years behind us and know that I can talk and even pray with them.



You guys are still doing great, and you may be happy for a long time without speaking to another soul, but please hear some advice – I'd rather have a few close friends that I can trust and share with than a ton of popular kids or the opposite – absolutely no one that I would call a friend. That would be unfortunate and it can change if you want it to.

What about you? How many people would you call a close friend? Do you have a best friend?

I challenge you to build up that courage, sit with someone at lunch, or at your place of worship, or at the next gaming convention, or find a group with like interests and say hello. Ask the person where they're from, what they like to do for fun, or what's their family like? You can do this and it is a risk to build great friendships, but it is also something I've seen create great reward! And if you need anything… support, advice, 100 percent confidential help, or someone to talk to, your Unit Ministry Team is here for you!

Cyber Skills, Teams Progressing

AUSA Magazine December 2018

The skills of Army National Guard and U.S. Army Reserve Soldiers have been an important part of the U.S. Army Cyber Command's success, the command's chief told a Senate subcommittee.

"Readiness of the total force requires that our investment in cyber ensures that active and Reserve and Guard forces are trained and equipped to one standard," Lt. Gen. Stephen Fogarty said.

The Army is making "progress toward fully integrating the Army's Reserve and National Guard into the cyber mission force," said Fogarty. "We're already benefiting from the critical skills the reserve component brings to bear and look forward to their full integration."

The Army's goal is to have 21 Reserve Component cyber protection teams: 11 in the Army National Guard and 10 in the Army Reserve.

Building partnerships between, federal, state, and private sector provides a whole of internet solution to cyber security:

By Frank Colon, Cyber Attorney Advisor, 780th Military Intelligence Brigade (Cyber)

Our adversaries, both nation state and criminal, have discovered that conducting offensive cyber operations against the U.S. in the "gray zone" has incapacitated the United States. The gray zone creates an ambiguous security and legal environment. The gray zone permits nation states and their bad actor proxies to conduct unprecedented theft of intellectual property and personal information for illegal gain. Nation states in particular have used the gray space to "…pursue their objectives while reducing the risk of triggering open warfare."

On a daily basis, hackers target businesses and individuals to steal corporate data or damage digital systems. In recent years, some foreign countries operate in close cooperation with cyber criminals and the dividing line between where a criminal enterprise ends and where a nation state begins is difficult to determine. Collectively these actors have no consequence when attacking private enterprise as American private enterprise can do nothing more than lock the doors and hope for the best. Currently, Federal Criminal Law prohibits U.S. companies who are under cyber-attack to "hack back" in order to thwart the attack. U.S. Statutes that lead to federal criminal charges for hacking are not effective against international hackers. Adding to the volume and complexity is the low cost of entry and lack of geographical boundaries.

Private businesses never anticipated that they would be forced to defend their operations from adversaries as capable as the foreign intelligence services of nation-states. Yet that is what they are forced to do in cyberspace. Unlike more traditional threats, cyber threats are so decentralized and numerous that the American government does not have the resources or bandwidth to be the sole provider of security in this realm. The legal and reputational constraints on the private sector's ability to aggressively and proactively defend itself thus creates a gap in the nation's cyber armor that exposes the integrity of private sector networks and data. If malicious actors were to take full advantage of this cybersecurity Achilles heel, such actions would seriously threaten national security, the economy, and privacy.

Jay Healey, senior research scholar at Columbia's School of International and Public Affairs said: "America's cyber power is not at Ft. Meade… NSA and U.S. Cyber Command are simply not positioned, and realistically can't be, to prevent attacks on private sector entities. By supporting capable businesses seeking to take proactive steps to defend their assets in cyberspace, the new administration can secure a cost-effective policy win with significant potential to improve whole-of-nation cybersecurity."

Given the inherent complexity of detecting nefarious cyber activities, a sole government solution cannot protect everyone on the internet. High costs and questionable effectiveness prohibit building of a cyber police force by the U.S. Government. Speed of relevance is critical to combating cyber-attacks. A whole of internet solution is required. Building quality partnerships between the whole of Government and Private Sector closes the gaps currently being exploited by our adversaries and will be essential to address the unrelenting onslaught of cyber-attacks against our Nation.

CTF All-Army CyberStakes

WINNERS

Cadet/ ROTC	Enlisted, E1-E4	NCO	Warrants	Officer	Civilian
CDT Sears Schulz	SPC Nick Polley	SSG Matthew Cundari	CW3 Ben Koontz	CPT Christian Sharpsten	Mr. Andrew Barbarello

Congratulations to the winners of the third annual All-Army Cyberstakes competition hosted by the Army Cyber Institute. More than 10,500 challenges solved and 1,125 folks competed, but in the end, there can only be one winner in the six categories.

Why I Stay...In the Fight!

FORT GORDON, Ga. -- *Sgt. Peter Yehl, an Arabic-Iraqi Linguist (MOS 35P), assigned t the 782nd Military Intelligence (MI) Battalion, reenlisted in the U.S. Army for four years prior to completing the Norwegian Foot March on November 3. (Courtesy photos)*

FORT GORDON, Ga. -- Sgt. Peter Yehl, from Akron, Ohio, is an Arabic-Iraqi Linguist (MOS 35P) assigned to the 782nd Military Intelligence Battalion (Cyber). Sgt. Yehl reenlisted for four years prior to completing the Norwegian Foot March on November 3. Yehl finished the 18.6 mile ruck march in 4 Hours and 13 minutes finishing 163rd out of 346 competitors.

The underlying reason for reenlisting was to continue to serve my country as a Non-Commissioned Officer and a Linguist, while at the same time seizing the opportunity to earn a second graduate degree.

My family was my biggest influence, as I always have to consider what CoA (course of action) best provides for a viable future.

My short term goals include earning certification in multiple work roles, completing the Master of Science of Strategic Intelligence program and teaching myself an additional language in support of mission needs. My long-term goals include earning a Ph.D. and retiring as a Chief Warrant Officer.

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

FORT BELVOIR, Va. *-- Sgt. 1st Class Michael Brothers, career counselor for the 782nd Military Intelligence Battalion (Cyber), is presented the U.S. Army Intelligence & Security Command (INSCOM) Career Counselor of the Year award by the INSCOM Command Career Counselor Sgt. Major Jorge Garcia. The event consisted of the Army Physical Fitness Test, a written examination testing each competitors knowledge of the Army Retention Program and the board appearance. Brothers will move forward to represent INSCOM at the Department of the Army competition. (U.S. Army photo)*

BALTIMORE *-- Sgt. Lord Larsen and Sgt. Juan Melendez, both assigned to D Company, 781st Military Intelligence (MI) Battalion (Cyber), reenlisted in the U.S. Army in front of friends, Family, and fellow Soldiers at the Federal Hill Park on Oct. 26. (U.S. Army photo)*

Cyber Soldier attains 'most prestigious credential

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

FORT GORDON, Ga. -- Master Sgt. Amanda Draeger, Cyber Operations Noncommissioned Officer-In-Charge, 780th Military Intelligence Brigade (Cyber), Fort George G. Meade, Md. (U.S. Army photo)

FORT GEORGE G. MEADE, Md. – A cyber operations non-commissioned officer (NCO) assigned to the 780th Military Intelligence Brigade (Cyber) here recently attained a level of cybersecurity certification few people in the world achieve.

Master Sgt. Amanda Draeger who hails from West Bend, Wisconsin, completed her GIAC Security Expert (GSE) certification from the Global Information Assurance Certification (GIAC) organization, making the master sergeant one of only four women out of approximately 250 people worldwide who are GSE certified, and one of just 15 certified DoD military and civilian members.

GIAC calls the GSE certification "the most prestigious credential in the IT Security industry." The organization says the unique hands-on, performance-based certification exam was developed by subject-matter experts and top industry practitioners to determine if a candidate has truly mastered the wide variety of skills required of top security consultants and individual practitioners.

Draeger serves as the NCO-In-Charge of the brigade's Joint Mission Operations Center, a major hub for Army and joint global cyberspace operations. She has a bachelor's degree in Information Technology with Security Emphasis and expects to complete her Master of Science in Information Security Engineering (MSISE) at the SANS Technology Institute in 2019.

"When you have 11 certifications from a single vendor, and that vendor provides a means of maintaining all of them at once just by obtaining one 'super-cert,' the super-cert becomes really appealing," said Draeger. "So I primarily sought it to reduce my own administrative overhead.

Additionally, the GSE is part of my MSISE which not only gave me extra incentive to pass, but gave me a community of support and extra resources to prepare."

"I spent about eight months preparing. The first few months were just reviewing and re-certifying the 'core' certifications … because they were about to expire. But this also provided excellent preparation for the written portion of the exam. My STI coursework also worked to prepare me by having me do hands-on challenges with NetWars (cyber operations exercise), as well as several written assignments. After the written exam, my STI faculty guided me towards some additional resources to improve analysis skills that were very useful for the lab portion of the exam."

Draeger said she can't really point to one person as her mentor, since so many people throughout her career have supported her along the way.

"The ones that I most try to model myself after are the ones that, when someone didn't know what was going on, saw an opportunity to teach," said Draeger. "Watching someone drop into teaching mode, without judging why the person doesn't know a thing, is one of the most amazing things to watch. It can be hard to, instead of doing everything yourself because it's faster, slow down and teach the next person what you're doing, why you're doing it, and how to do it, but that is how we grow and mature the force."

Along with those mentors Draeger said she has some role models in the cyber world that she admires.

"A couple of specific people I look up to are Katie Moussouris and Chris Sanders," said Draeger.

in the IT Security industry'

"Katie is one of those people who leans on her technical expertise to try to fix policy. She's testified in front of the U.S. Senate Subcommittee on Consumer Protection, Product Safety, Insurance, and Data Security about security research for defensive purposes, and has done work on getting exemptions for security researchers in the Wassenaar Arrangement. Chris, on top of the amazing books he's written and training he's produced, has done a ton of work with the Rural Technology Fund, which gets technology kits in the hands of schools in rural areas that otherwise wouldn't have access to that tech, which is a cause near and dear to my heart."

QUICK SKETCH:

-- Enlisted as an Information Technology Specialist (MOS 25B), later transitioned to be a Cyber Network Defender (MOS 25D), and then converted to her current MOS one year it was introduced her position.

ON WHY SHE CHOSE THE ARMY:

"I joined the Army primarily because I needed a job. I've always been interested in computers, but between the fact that my rural school didn't have much beyond 'how to use computers' and there was no plan for funding college, finding skilled work was hard. So I saw the Army as way to get some formal training, get a resume started, and get some money I could use for college. I succeeded at all of those goals and found out that I get along pretty well with the Army, so I've hung around."

ON WHY SHE CHOSE ARMY CYBER:

"I 'grew up' in the Army Signal Corps. I learned that we are extremely good at making systems work, even when we don't have all of the ideal resources. However, we have historically been less good at 'architecting' systems that are resilient, that are easily defensible, and ensuring that the people maintaining those systems have enough understanding to make them work better. Being part of the Cyber workforce means being in a position to improve the foxhole, to help the force as whole to get better at their jobs, and to develop deeper expertise that I wasn't able to get while I was Signal."

ON WHAT SHE WOULD TELL SOMEONE CONSIDERING ARMY CYBER:

"Be prepared for both excitement and terror. It's exciting because you get to shape the future and build something from scratch, which is an opportunity you don't get very often. It's terrifying because it is up to you to shape the future, and you have to build things from scratch.

"INFOSEC (Information Security) is a huge, huge world. There are a ton of different areas that you can specialize in, from forensics, to malware analysis, to the intricacies of (Industrial Control Systems/Supervisory Control and Dada Acquistion) environments. ... If you're interested, there's a place for you. Don't be scared off by all the technical stuff. That's the easy part. If you want to learn; if you want to solve real-world problems; I can teach you the technical parts, regardless of your background. If you enjoy being a perpetual student, Infosec is some of the most fun you can have."

ON WHAT CERTIFICATION MEANS:

"I have the ability to not just execute technical tasks, but I understand what is actually going on under the hood, and I'm able to communicate that to both a technical audience and a managerial audience. It is that particular combination of requirements that makes the GSE so difficult, and so respected. I'm not going to say that being a GSE is a cure for impostor syndrome, but it certainly helps."

ON HER FUTURE GOALS:

"My immediate goal is finishing out my master's. Given that I come from a family where the most educated person has an associate's degree, that alone is a huge accomplishment. As far as the overall arc of my career, I see a critical gap in people that are both highly technical and able to talk policy and strategy. If we are going to have legal and policy support for what we do, we need to be able to communicate our needs with the people who create the way ahead."

ON HER FAVORITE QUOTE:

"If you torture the data long enough, it will confess to anything" – Darrell Huff (How to Lie with Statistics) (also attributed to Ronald H. Coase) "This is a really good reminder to anyone performing analysis to not force one's biases on the data."

Cyber Blitz 2018

Continued from page 12

"It's a new frontier for the MI discipline within the Army and we get to address these questions, we get to think about discussions in an abstract way and try to inform doctrine going forward."

Sanders explained, in addition to validating the CWSB construct and the ECT model, ARCYBER was integrating the Army's vision for multi-domain operations to inform the U.S. Army Pacific (USARPAC) multi-domain task force (MDTF) on how fight in the cyberspace and the EW domain. The ICEWS (Intelligence, Cyberspace, Electronic Warfare and Space, pronounced I-Qs) detachment is a new unit being formed under the 17th Fires Brigade, and Sanders explained the Army doesn't have to wait for it to be fully manned – CB18 and future USARPAC exercises can inform the process now.

All of the CB 18 participants came away with valuable lessons learned to take back to their commands which will also benefit the Army by providing an overmatch in capabilities against a regional peer in a potential future fight.

"What excites me is that we are at the forefront of technology to be able to increase the lethality of the brigade combat teams, divisions and corps of the Army," said Sanders. "We are looking at the wave of the future for how the Army is going to fight multi-domain operations using and leveraging technology. Being able to test that out here at Cyber Blitz and bring that to the brigade-level is pretty amazing."

TFE NCO Induction

Continued from page 26

"I really see them doing cyber assessments and protection testing for different corporations and government agencies within the state," said Nip. "The (Adjutant General) has already come out and said election support. I see that type of activity, bringing this together to help the state understand how we can provide a capability to state government and the governor of the state."

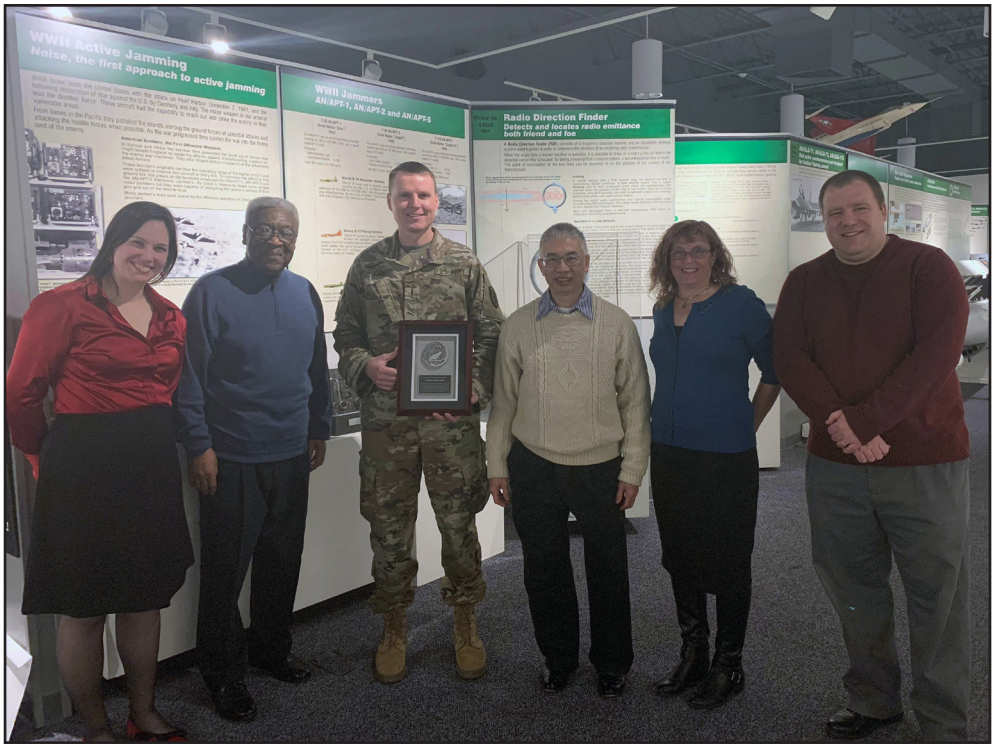
Gen. Jeffrey Burkett, vice director of Domestic Operations, NG Bureau, appreciated the opportunity to attend the event and said, "Thanks for putting on a great DV visit. I learned a lot and have a much deeper appreciation of the Task Force Echo mission, opportunities, and challenges.'

The distinguished visitors included Lt. Gen. Fogarty; Gen. Burkett; Command Sgt. Maj. John Sampa, ARNG; Maj. Gen. Robert Livingston Jr., the Adjutant General, S.C.; Command Sgt. Maj. Russell Vickery, S.C. NG; Col. Ronald Taylor, chief of staff, S.C. NG; Brig. Brig. Gen. Timothy LaBarge, chief of staff, New York Air National Guard; Command Chief Master Sgt. Amy Giaquinto, state command chief, N.Y. NG; Brig. Gen. Rodney Painting, assistant Adjutant General, Louisiana NG; Command Sgt. Maj. Darren Delrie, Louisiana ARNG; Col. Nip; Col. Jeffrey Eget, commander, 57th Troop Command, N.J. NG; Col. Teri Williams, deputy commander, 91st Cyber Brigade, Virginia ARNG; Command Sgt. Maj. Daryl Plude, 91st Cyber Brigade; and Maj. Chris Winnek, Joint cyber operations chief, Texas Military Department and G6, 36th Infantry Division, Texas NG.

FORT GEORGE G. MEADE, Md. – *The senior leaders of the 780th Military Intelligence Brigade (Cyber), as well as other garrison tenet unit leaders, took part in the military's tradition of 'serving those who serve', on Thanksgiving day at the Freedom Inn dining facility. In dining facilities across the U.S. and around the world, you'll find military leaders serving those who serve. (U.S. Army Photo)*

2018 Army Outstanding Unit Award

ODENTON, Md. – *Chief Warrant Officer 5 Travis Ysen, the senior technical advisor for the 780th Military Intelligence Brigade (Cyber) accepts the Army Outstanding Unit Award from the Association of Old Crows (AOC) on behalf of the Soldiers and Army Civilians of the Brigade. The outstanding unit award recognizes meritorious and distinctive sustained performance by a military unit (Army, Air Force, Navy, Marines, Coast Guard, and International) in advancing or exemplifying the discipline of Electronic Warfare. The award recipients are selected by the Service chiefs who may select one unit along with evidence documenting the nominee in the previous calendar year. Additionally, the actions of the nominee must have had a significant impact on the warfighter. (Courtesy Photo)*



780th Military Intelligence Brigade

For exceptionally meritorious service for furthering the advancements and the strategic vision of the Cyber domain and Electronic Warfare in support of the national defense. The 780th Military Intelligence Brigade championed the CSA's CSCB pilot program. Provided unprecedented worldwide offensive Cyberspace Operations in support of Army Combat Commands, Department of Defense, and Interagency Operation. The extraordinary accomplishments of the 780th Military Intelligence Brigade reflect great credit upon the unit, United States Army Intelligence and Security Command, United States Army Cyber Command, and the United States Army.

Commander's Cue: Deterrence

Continued from page 1

As members of the Nation's Cyber Mission Force, our Brigade plays a critical role in deterrence. Our unparalleled technical skills and professionalism ensure that USCYBERCOM is capable of delivering effects against any adversary in and through cyberspace. Our agile, adaptive, and opportunistic mindset guarantees that should be we called to act, we will not fail; we will seek and use every opportunity and advantage in both attack and defense.

We are ready – trained, equipped, and manned to not only deter, but defeat any adversary in and through cyberspace. We are the "known unknown," and we are ***Everywhere and Always, in the Fight!***

Brigade Vision Statement:

We are America's most innovative cyberspace operations force, deterring, and when directed, defeating our nation's adversaries in and through cyberspace

Senior Leader Quotes

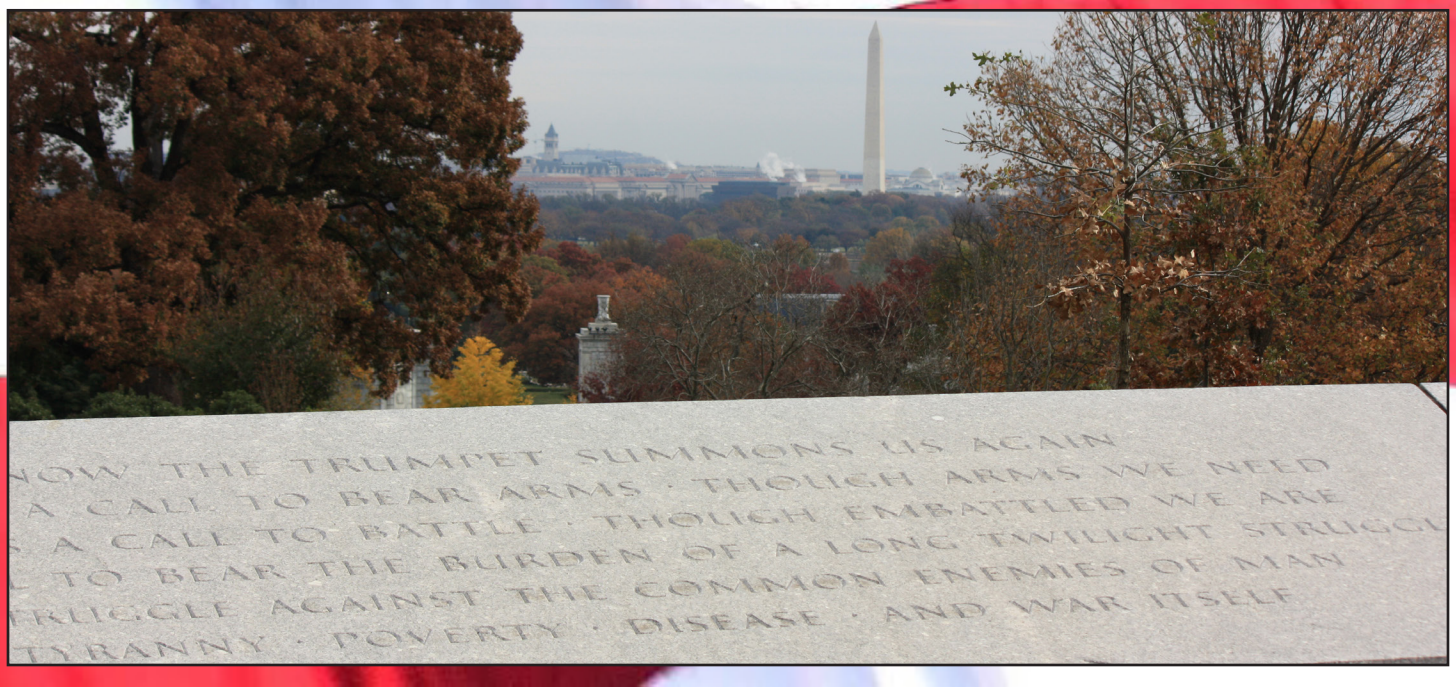
"When our nation asks, 'What function does U.S. Cyber Command (USCYBERCOM) perform that obligates society to assume responsibility for its maintenance?' the command can reply that its strategic concept has evolved from a 'response force' to a 'persistence force.' This persistence force will contest our adversaries' efforts in cyberspace to harm Americans and American interests. It will degrade the infrastructure and other resources that enable our adversaries to fight in cyberspace. Over time, a persistence force, operating at scale with U.S. and foreign partners, should raise the costs that our adversaries incur from hacking the United States. To protect our most critical public and private institutions from threats that continue to evolve in cyberspace, we cannot operate episodically." -- *Gen. Paul M. Nakasone, commander of U.S. Cyber Command, director of the National Security Agency, and chief of the Central Security Service, excerpt from "A Cyber Force for Persistent Operations", Joint Force Quarterly, Issue 92, 1st Quarter 2019*

"The Army's philosophy for training is to 'Train as you fight!' For the Army's teams within the DoD's Cyber Mission Force (CMF), training to a joint standard is predicated on a culture of adaptive learning, where operations inform training at every level."

"With the achievement of Full Operational Capability of the Army CMF, the Army and Joint Force are shifting focus to measuring and sustaining CMF readiness. Readiness of the CMF's ability to conduct cyberspace operations reflects a teams' ability to plan; develop access; report and maneuver in cyberspace; hold targets at risk; and deliver capabilities based on assigned missions; this is the standard we use for training. This includes a focus on non-standard access methodologies, Title 10 operator training, and integration with mission partners to improve mission readiness." -- *Lt. Gen. Stephen G. Fogarty, commander, U.S. Army Cyber Command, statement before the Subcommittees on Cybersecurity and Personnel Committee on Armed Services U.S. Senate, September 26, 2018*

Veterans Day 2018

ARLINGTON, Va. *– On behalf of the Soldiers and Civilians f the 780th Military Intelligence Brigade (Cyber), the brigade leadership participated in a wreath laying ceremony at the Tomb of the Unknown Soldier at Arlington National Cemetery in order to show our respect for those who serve and for those who paid the ultimate sacrifice in observance of Veterans Day on November 12. (Courtesy Photos)*



FORT BELVOIR, Va. – FORT BELVOIR, Va. – Spc. Alexander Musarra, 782nd Military Intelligence Battalion (Cyber), from Miami, receives the Army Commendation medal from Maj. Gen. Gary W. Johnston, commanding general, U.S. Army Intelligence & Security Command (INSCOM), for his selection as the INSCOM Soldier of the Year following the INSCOM-level Best Warrior Competition in August 2018. Musarra, an Iraqi Arabic Cryptologic Linguist (MOS 35P), is also the 780th MI Brigade (Cyber) Linguist of the Year. (U.S. Army photo by Jocelyn Broussard)