Volume 7, Issue 3

the BYTE

780th Military Intelligence Brigade

* Army activates 915 Cyber Warfare Battalion
* AvengerCon IV "Goes Big"
* "Hackathon" supports STEM
* SANS NetWars

Disciplined Initiative & Risk Acceptance

PRAETORIANS

780th MI BDE

"STRENGTH AND HONOR"

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:
FORT GORDON, Ga. *– On May 22 the 915th Cyber Warfare Battalion made U.S. Army history when this tactical unit encompassing cyber operators, electronic warfare, information operations, and signalers, unfurled their colors for the first time in an activation ceremony. The unit is assigned to U.S. Army Cyber Command, and operates under the 780th Military Intelligence Brigade (Cyber). (US Army Photo)*

Features

Articles

From the Editor

The theme for this issue of the BYTE is *"Disciplined Initiative and Risk Acceptance"*.

In accordance with ADP 6-0 Mission Command, the Army defines Disciplined Initiative as "action in the absence of orders, when existing orders no longer fit the situation, or when unforeseen opportunities or threats arise." The Army defines Risk Acceptance as a "deliberate exposure to potential injury or loss when the commander judges the outcome in terms of mission accomplishment as worth the cost."

Each company command was challenged by the brigade commander to submit an article representing his/her command and to put their "best foot forward". The commander could either write the article themselves, contribute or ask someone else to. The topic could incorporate historical examples relevant to cyber operations, or could even deliberate on why black hat (white or grey hat) hackers don't seem to have these discussions.

"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

Disciplined Initiative & Risk Acceptance

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

World War I was one of the bloodiest wars in history. In a short four years, almost ten million combatants were killed and over 20 million wounded – a scale nearly impossible to comprehend compared to contemporary conflicts. But even within this meat grinder, some battles were so horrendous that they stand out as exceptional. Verdun, a city in northern France, was one such battle. The battle of Verdun was – by design – intended to be a battle of attrition. Lasting more than 300 days, it was the longest battle of the war. Casualty rates were so high that burials were rare and frequently unsuccessful; the massive use of artillery (40-60 million rounds fired) meant that most of the dead buried on the battlefield were violently disinterred. Even today, remains are frequently found at Verdun; the battlefield's ossuary holds the mixed bones of over 130,000 French and German soldiers whose names will never be known.

But even within this cacophony of artillery and bloody slaughter, the German army executed mission command (auftragstaktik) on a daily basis – including at the tactical level. And it was at the tactical level that one of the greatest examples of the principles of disciplined initiative and risk acceptance occurred.

Critical to the French defenses at Verdun was Fort Douamont, the largest and highest of nineteen forts which protected the city. The fort was widely considered one of the strongest in the world at the time. Boasting numerous turrets, including a retractable 155mm gun, the fort was protected from artillery by nearly 40 feet of steel-reinforced concrete. In addition to fields of barbed wire and trenches, the fort was also surrounded by a dry moat 24 feet deep and 35 feet wide, with anti-personnel cannons and machine guns poised to shoot anyone foolhardy enough to enter it. When fully manned, the fort was near impregnable.

However, before the battle the French made a grave mistake. Believing that German heavy weapons could easily destroy the fort and having need for the resources elsewhere, they removed most of the fort's heavy weapons and left it minimally manned.

On February 21, 1916, the Germans launched the offensive that would become the Battle of Verdun. They made rapid progress; by the 25th of February, a reconnaissance element of the 24th Brandenburg Regiment approached Fort Douamont. What they didn't know is that the Fort's garrison had been reduced to only 56 soldiers, and that the only turret manned was the 155mm gun which was focused on long-range German targets.

Continued on page 3

Aerial photograph of Fort de Douaumont, Verdun, 1916. (Public Domain at https://en.wikipedia.org/wiki/Séré_de_Rivières_system#/media/File:Douaumontfort.jpg)

Disciplined Initiative & Risk Acceptance

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

This quarter's newsletter topic is disciplined initiative and risk acceptance. In the spirit of this topic, I am going to take some disciplined initiative, accept some risk, and go off topic.

What I want to talk about are the amazing accomplishments of our organization and the people that make them possible, you. I have just surpassed the two year mark serving as your Brigade Command Sergeant Major and I continue to be amazed and proud of the great things you do. We continue to lead the way in getting after the mission and taking care of our personnel. We must continue to do so. Without our personnel, we would not be able to accomplish our mission. It isn't just the cyber teams, it is the organization as a whole, to include the supporting staff. Sure there are hiccups along the road, but once identified, we come together to solve the issue and get back on track. For this I am grateful. You really make my job easy and fun.

I am constantly in awe of everything this Brigade does on a daily basis. You pave new ground for the Army and Department of Defense on a regular basis. You establish new and improved processes for both the Intelligence and Cyber communities. Everything you do has the potential to have ground-breaking implications. From the day-to-day things like processing awards, nominating personnel for access, writing operations orders, ordering equipment, and establishing computer accounts to gathering intelligence and operating in cyberspace, this Brigade is on the leading edge and the people in this unit strive to do the best they can do every day. That is all anyone can ever ask.

Over the last two years, I have witnessed this and frequently hear the accolades of senior leaders from across the Department of Defense regarding the work you do. The reason for this high praise is you. You are the ones that do the heavy lifting to accomplish the Brigade's mission. Without you, this unit would not be successful. I am proud to serve and to serve with each and every one of you. I could not have asked for a better unit or group of people to work with as my last assignment in the Army. Thank you for everything you do.

Okay, so maybe I will get back on topic and mention disciplined initiative and risk acceptance. Whether or not you know it, you exercise this every day. It isn't just the risk and initiative some use when trying to prevent detection when going after an adversary. It is also the risk acceptance and disciplined initiative that you use to get after the changing team and mission requirements, external training requirements, or the everyday things you do to take care of personnel and accomplish the mission. In reality, this is a very good topic for our organization and our mission. We need the Soldiers, Civilians, and contractors of this organization to take the initiative and make things better. Only if we work together will this unit continue to exceed all expectations and lead the way by accomplishing our mission and setting the standard for others to emulate.

Thank you for everything you do. It is my greatest pleasure to serve you.

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

FORT GEORGE G. MEADE, Md. – *Command Sgt. Major James Krog, the senior enlisted leader for the 780th Military Intelligence Brigade (Cyber), was the guest speaker at a Noncommissioned Officer Induction ceremony at the Post Theater on October 16. (U.S. Army Photo)*

Disciplined Initiative and Risk Acceptance (cont.)

Continued from page 1

Pioneer Sergeant Kunze

Leading a small squad of sappers was Pioneer Sergeant Kunze, a 24-year old noncommissioned officer (NCO) from a poor family. Sergeant Kunze's mission was to remove all obstacles in the path of the attacking infantry, and he was briefed to not advance any further than the objective.

Maneuvering across the battlefield, Kunze and his squad came upon Fort Douamont – the largest and most formidable obstacle on the battlefield and most certainly not the objective for the 24th Brandenburg. More interestingly, the Fort seemed silent.

Did Sergeant Kunze stop, check his map, and retreat because Douamont was not listed in his Mission Profile? Did he see the turrets, believe the risk was too great, and choose inaction?

No. Pioneer Sergeant Kunze executed disciplined initiative, assumed risk, and disobeyed his orders. Kunze understood the Commander's Intent, and realized that his orders no longer fit the situation. There was an opportunity, and because the German Army executed auftragstaktik (mission command) he knew he was expected to take action and develop the situation. Sergeant Kunze accepted the risk of attacking the fort, even knowing there was no way to know the fort was minimally manned. The opportunity was too great to ignore, and all opportunities come with risks.

Sergeant Kunze and his squad approached the fort and slid down a damaged wall into the bottom of the moat. Facing them from both sides were two gun emplacements, engineered with clear fields of fire. Accepting the risk, they advanced to one end of the moat, reaching the base of one of the emplacements. Sergeant Kunze directed his squad to build a human pyramid to lift him and two other soldiers into the firing port of the gun emplacement twelve feet above the bottom of the moat. They were in.

Sergeant Kunze had successfully breached the strongest fort in the world without his squad suffering a single casualty.

Immediately upon entering the fort, he began clearing it. At a turn in the passageway, he left the two accompanying soldiers to guard it and advanced forward alone. The first door he found turned out to be the 155mm artillery team, whom he captured and started to escort through the fort. Getting lost in the maze of tunnels, the prisoners soon ran from their captor. Giving chase, Kunze's search soon led him to another room where an NCO was teaching a class to 20 other soldiers. He raised his weapon, took them prisoner, and locked them in the room. Continuing his search, he soon happened upon the kitchen where, after days without a good meal, he sat down and ate.

While Kunze ate, other German forces found the fort and gained entry. Within hours, the fort was formally in German hands. The greatest fort in the world, and the keystone to the defense of Verdun, was captured without a shot fired or casualty taken.

Douamont wasn't taken because of a detailed plan that addressed every possible risk, briefed to and approved by the senior leaders of the German Army. Douamont was taken because a single NCO executed mission command. Douamont fell because Pioneer Sergeant Kunz exercised disciplined initiative and accepted risk.

The capture of Fort Douamont was not only a massive propaganda victory for the Germans, it was an incredible loss for the French. The Fort served as a forward, protected base for German forces throughout the battle, and its dominating position on the battlefield enabled German defenses throughout the fight. Ultimately, Douamont was recaptured, but at great cost to French forces. An estimated 100,000 French fell to recover what a German NCO had captured without a single bullet fired.

Continued on the next page

Continued from previous page

What can we learn from a single NCO who fought in a battle over a hundred years ago? First, that no opportunity comes without risk, that risk is impossible to avoid in military operations, and that leaders at every level must be prepared to assume prudent risk. Second, that mission command requires us to take advantage of unforeseen opportunities when existing orders – often based on limited intelligence and faulty assumptions no longer fit the situation.

Every leader is expected to execute disciplined initiative and assume prudent risk. It is foolish to argue that we must be more risk adverse in the conduct of cyberspace operations than we are in the execution of conventional operations. Mission command is – and will remain – a foundational element in successful Joint and Army operations, and leaders at every level must be prepared to underwrite the risk their subordinates incur in its execution.

Epilogue: Sergeant Kunze was never recognized as the conqueror of Douamont during World War I. Instead, one of the officers that followed him into the Fort became a German hero. It took 20 years for Sergeant Kunze's role in the attack to be fully understood. When asked why he never complained nor took issue with his lack of recognition, Sergeant Kunze's answer epitomized his internalization of auftragstaktik. He was afraid that admitting he had paused to eat would have brought him censure instead of honor. His strict interpretation of mission command required that he press the attack and continue to pursue additional opportunities. He was embarrassed to admit that he had paused the attack to fill his belly. Finally receiving belated recognition for his efforts, Sergeant Kunze was awarded the Pour le Mérite.

Praetorian 6
"Strength and Honor"

Pour Le Merite, "Blue Max", the highest honor presented to Germans in WW I

AUGUSTA, Ga. -- Senior leaders of the 780th Military Intelligence Brigade (Cyber) visited the Georgia Cyber Center for a tour and a briefing by the Defense Digital Service and Cyber Center of Excellence on December 5. (U.S. Army Photo)

A Nibble on Disciplined Initiative

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

As I thought about Disciplined Initiative and Risk Acceptance, I began to wonder why we struggle with the concept and implementation. To help refine the problem, I asked myself the following questions:

- How comfortable is the workforce with operating under these conditions?
- How prepared is the workforce to execute disciplined initiative?
- How risk-tolerant is leadership?
- Is there a trust barrier between the workforce and leadership regarding executing mission within a broader risk quotient?

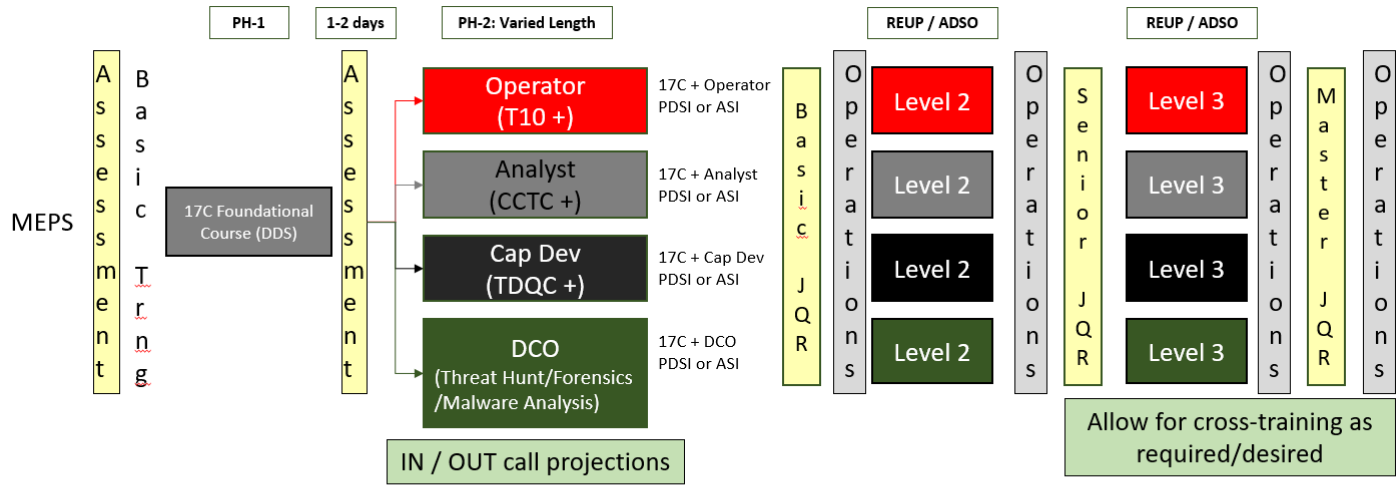
While I don't have the answers to all, if any, of these questions, I believe that a portion of the solution lies in how and when we train our personnel.

The 17-series Career Management Field (CMF) was partially established on the principle that a single MOS (military occupational specialty) could execute offensive and defensive cyberspace operations (OCO/DCO) to a high degree of proficiency. To achieve this, a common-track training program was developed at the schoolhouse and a practice of cycling personnel between OCO and DCO assignments was implemented. The main premises being that each focal area shares common knowledge, skills, and abilities (KSAs) and that, over time, the force would become highly proficient across the domain. However, cyber is a vast area of study that demands focused training, education, and years of employment within a particular specialty to build mastery. Under the current training and employment model, mastery is more of a distant goal rather than an achievable reality. While pockets of excellence in the force exist, they are sporadic and difficult to maintain in a repeatable manner. To remedy this, I propose the following precepts be established:

- Cyber employment is generally broken into the following bins: Operator, Analyst, Capability Development, and Defense (Host and Network)
- A one-size fits all training path is not conducive to professionalization
- Professionalization within a specialty should be encouraged and facilitated
- Early identification, selection, and training within a specialty is required
- Assignments should be sequenced to build experience within a specialty area
- Offensive and defensive missions should not be wholly separate, but have consolidated operations centers where coordination and fusion are the norm

One potential approach is to divide the 17-series into individual MOSs that focus on the core tasks of analysis, operations, capability development, and defense. However, splitting an MOS population into smaller components diminishes its viability, leading to a lack of upward mobility and stagnation. An alternative is to develop professionalization tracks across the 17-series MOS, similar to the model employed for linguists. A tracked career model would enable personnel to focus on a particular specialty, leading to mastery over the course of their career.

Another area linked to the operational force attaining mastery is the identification, selection, training, and employment of talent as it aligns to individual strengths. Under the current model, enlisted and officers attend a single block of training prior to entering the operational force. The training is designed to provide a technical foundation that enables the operational force the latitude to employ personnel across a range of OCO and DCO work roles. While this provides operations with a slate of personnel to work with, it doesn't do well with setting a course for professionalization within a specialization. Implementing a model similar to Figure 1 would enable the early identification of talent, as well as an ability to focus in a given specialty over the duration of a career.



An adjustment to the training path, starting with the Cyber School, would better position the operational force to fill and execute its operational needs. This adjustment would also enable professionalization in specific concentration areas rather than individuals being responsible for the totality of Cyberspace Operations. That said, cross training should be encouraged as required. However, focused energy should be expended to professionalize within a concentration area in an effort to achieve master-level proficiency.

Figure1: Selection starts as early as MEPs via a Cyber Assessment that evaluates knowledge and hands-on skills.

Recently, Defense Digital Services (DDS) developed and piloted a course intended to be an alternative to the Joint Cyber Analysis Course (Phase 1 of 17C Advance Individual Training). This new Phase 1 course, once implemented, could serve as a common-core training for all 17Cs. Following Phase 1, personnel could be issued an assessment that determines the follow-on track (Operator, Analyst, Capability Developer, or Defense). Phase 2 would be of varying lengths depending on the complexity of the required training. Ideally, much of the existing course ware would be leveraged (Title 10 BOC (Basic Operating Course), CCTC (Cyber Common Technical Core), and TDQC (Tool Developer Qualification Course)) to minimize development efforts. Additional training would need to be developed to meet DCO host and network requirements involving threat hunting, forensics, and malware analysis concepts. Level 2 and 3 training would need to be developed to ensure Senior-level criteria are addressed. However, current training for operators and analysts could be leveraged, further reducing development requirements. While this model requires significant development and/or refinement of current training, it provides a means to achieve professionalization; something that is lacking under the current model.

Currently, cyber is effectively bifurcated into two distinct mission sets that are separated by function and space (780th Military Intelligence Brigade (Cyber) and the Cyber Protection Brigade). Each mission is wholly separate, discouraging coordinated effort outside of the occasional exchange of personnel during move cycles. This employment method fails to embrace the premise that cyber was formed to accomplish both missions under a single umbrella. It also fails to facilitate mastery level professionalization within specializations (mastery requires deep knowledge and skill within a specialty, but also an understanding of how the specialty relates across OCO and DCO missions). A concern with a tracked employment model is a further stove piping of information and granular separation of OCO and DCO missions down to the individual level. To overcome this, OCO and DCO should be collocated within the same operations floor where practical. Sharing of information should also be facilitated through the employment of common databases and reporting. An operations floor that employs OCO, DCO, Intelligence, and Capability Development assets would facilitate mission cooperation. This coupled with a tracked model enables personnel to gain depth within specializations while expanding their experience across OCO and DCO missions.

Continued on page 40

Disciplined Initiative, the Pivot, and You.

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

Mission Command principles, especially disciplined initiative and risk acceptance, are essential characteristics of both a successful battalion and an operationally effective Cyber National Mission Force. Our recent pivot has tested how we implement these principles, and upon reflection I remain humbled and honored by the battalion's initiative, innovation, and progress in the last quarter.

This article is another opportunity to re-emphasize my philosophy in the context of our new decentralized nature and greatly expanded mission.

While we are all based in the Fort Meade area, we have always been dispersed across geography and mission. However, since our pivot, this decentralization is even more exaggerated. I am now routinely physically separated from our Command Sergeant Major, S3 (operations), and executive Officer, and logically separated from most of the operational missions of our teams. Given our more dispersed environment, I am more reliant on my intent and philosophy to set our culture, expectations, boundaries, and objectives. Our success then rides on the disciplined initiative of our leaders, including NCOICs (noncommissioned officers-in-charge), sub-element leads, deputies, chiefs, corporals, staff—everyone!

This style *only* works well with high-performance leaders who are smart, well-informed, and empowered. Whether as a leader you leverage it or not, I have empowered you since day zero with a focus on teaming, transparency, optimism, and fact-based decision-making. These are the essential building blocks that companies, teams, and sections should use in pursuit of the mission. I trust you to do the right thing at the right time with the right urgency. Since assuming command, I consistently emphasized a culture that develops leaders with the confidence and skills to fully execute disciplined initiative: decisive, positive, and productive action in the absence of direct guidance.

Initiative is both tempered and enabled by risk acceptance. Risk acceptance and risk aversion are contradictory, and coming to terms with risk is perhaps our greatest operational challenge. This battalion operates under a unique framework that is intended to support flexible task organization. However, this framework operates inside a much larger, much older system that competes with itself to balance new against old, control against speed, effects against endurance, and focus against coverage.

Take notice of the strong winds now at our back. This is our time to rise over old obstacles, build new expectations, gain new ground, and impose true costs. Work together and make it happen. We have everything we need right here.

We got this!

VANGUARD 6.

"Vanguard...When Others Cannot!"

COLUMBIA, Md. *– Lt. Col. Nadine Nally, commander of the 781st MI Battalion, presents her challenge coin to Daniel Cuthbert, the keynote speaker at this year's AvengerCon at the DreamPort facility on October 17. (Army Photo)*

Surge Operations: A Deployed-In-Place Unit Dilemma

By Lt. Col. Wayne Sanders, commander, 782nd Military Intelligence Battalion (Cyber)

Here in the 782d Military Intelligence Battalion (Cyber), we support four operational headquarters globally. While an incredible honor to support these amazing commanders, it comes at a steep price… the demands never stop. As the Mighty Cyber Legion's reputation continues to soar and our successes continue to pour in, these commanders continually want more and more cyber.

For those of you who come from FORSCOM (U.S. Army Forces Command) units, you may remember something called Block Leave. This is a designated time (normally two to three weeks) set aside by the Commander to shut down the entire battalion for rest, relaxation, and reset. People can forecast six months in advance to take family vacations, plan reunions, or take epic road trips. Prior to becoming Cyber, my wife Kira and I took a road trip from Fort Lewis Washington, to Disneyland, to Las Vegas, and onward to Tucson, Arizona. We met up with friends and family, and we had a blast!

However, if you command a unit that is 24/7/365 in support of several different operational commanders, you can't just tell them that the Cyber Legion is taking a break this July. We are expected to be ready to answer the commanders' call whenever that bell rings. Additionally, as demanding and specialized as the Cyber Branch is, many times we have only one or two people that can accomplish a specific task. And while the work that we do is fascinating and one of a kind, it is not sustainable to surge every minute of every day.

In an effort to ensure that we maintain our edge and continue pushing the envelope, I have challenged my command teams to come up with innovative solutions to address the "burnout problem." This takes place in a lot of different ways:

- Identify breaks in surge operations to allow Soldiers and Civilians to take leave.
- Give personnel an opportunity to partner with the Cyber School and teach "on podium" to the younger generations on an ad hoc basis.
- Plan key family morale events so the families are fully aware of the importance of balance
- Partner with Georgia Cyber Center and Defense Digital Services to get a new and innovative look at different technologies
- Enroll in SANS classes to continue educating our experts

These are only a few of the many ideas that the Cyber Legion Leaders are looking at to address this issue. The key here is the ART OF LEADERSHIP. None of these solutions will satisfy all Soldiers and Civilians that are approaching burnout…the key for all of this is: KNOW YOUR PEOPLE! What motivates them? Is it family time? Is it a technical edge? Is it a new challenge? No matter what it is, our leaders must proactively seek new solutions while balancing the demand from the operational leadership.

This will be a continuing problem with many solutions, but no matter what, we will continue to look for whatever remedies are necessary to keep the Cyber Legion as the most sought after battalion in the entire Cyber Branch!

"Cyber Legion, Silent Victory!"

Battalion helping shape Army tactical capabilities in the

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

***FORT GORDON, Ga.** – The 915th Cyber Warfare Battalion made U.S. Army history when this tactical unit encompassing cyber, electronic warfare, information operations, psychological operations, and signal intelligence Soldiers, unfurled their colors for the first time in an activation ceremony on May 22. (U.S. Army Photos)*

FORT GORDON, Ga. – The U.S. Army activated the 915th Cyberspace Warfare Battalion (CWB) in May 2019 to help meet the Army's current and projected tactical Cyberspace Electromagnetic Activities (CEMA) requirements.

The 915th CWB, through its Expeditionary CEMA Teams (ECTs), provides a scalable capability to deploy Expeditionary Cyberspace Operators to conduct operations to deny, degrade, disrupt, destroy and manipulate cyberspace effects for Army maneuver commanders at the Army Service Component Command level and below.

The origins of the 915th CWB date back to 2015, when U.S. Army Cyber Command's (ARCYBER) CEMA Support to Corps and Below pilot program began helping to shape the Army's ability to fully integrate cyberspace, electronic warfare (EW), information operations (IO) and tactical signals intelligence (SIGINT) operations with fires and protection at the Army corps level and below in support of Multi-Domain Operations. The Army, at theater army and below, was challenged to deny, destroy, degrade or disrupt adversary use of the electromagnetic spectrum.

In June 2019, as a result of the pilot's findings, the Secretary of the Army ordered ARCYBER to build a Cyberspace Warfare Battalion in the Army's active force.

The 915th CWB falls under the operational control of ARCYBER; but command authority and administrative control of the battalion falls to the 780th Military Intelligence (MI) Brigade.

Col. Brian Vile, commander of the 780th MI Brigade, said the battalion exemplifies the ARCYBER motto of "Attack! Defend! Influence!"

"The 915th is assembling the most technically gifted Soldiers, putting them into the most challenging

***HOHENFELS, Germany** – Soldiers assigned to the Expeditionary Cyber Team, 915th Cyber Warfare Battalion, supported the 1st Infantry Division at Saber Junction 2019 and were able to dominate the information environment.*

HOHENFELS, Germany – *Soldiers assigned to the Expeditionary Cyber Team, 915th Cyber Warfare Battalion, supported Saber Junction 2019 at the Joint Multinational Readiness Center in September in order to plan and organize the integration of information warfare strategies and tactics.*

environments, and asking them to figure out new ways to employ technology and information to deliver effects in the physical, virtual, and cognitive domains," said Vile. "We won't tell them how to operate; instead, we'll tell them what needs to be done and ensure they have the tools and authorities to do it."

Just months after the battalion's activation, one of its ECTs deployed to the Army's Joint Multinational Readiness Center in Hohenfels, Germany in support of exercise Saber Junction 2019, a large-force exercise involving nearly 5,400 participants from 16 allied and partner nations.

2nd Lt. Shane Neal, an Offensive Cyber Operations planner with the ECT, was part of a cyber planning cell integrated into the training brigade's plans staff during the exercise. Neal said Saber Junction was an opportunity for the ECT to plan and organize the integration of cyber warfare strategies and tactics, assigning CEMA technologies to battlefield operations.

At Hohenfels the ECT provided direct CEMA support to the 1st Infantry Division. Capt. Adam Schinder, the ECT commander, said the team was able to dominate the information environment across the entire JMRC network, enabling remote cyber operators at Fort Gordon to exploit and dominate the network, and effectively integrate cyberspace and information operations.

The 915th CWB is expected to double CEMA support, from two to four training rotations per year, at the Army's Combat Training Centers at Fort Irwin, Calif., and Fort Polk, La., and improve the readiness of Army maneuver units to defend cyber key terrain and exploit cyberspace opportunities.

"ECTs allow for additional options and capabilities for commanders to integrate into their scheme of maneuver and fires plan, to deliver effects at the timing and tempo needed by the tactical echelon," said Lt. Col. Matt Davis, commander of the 915th CWB.

According to Maj. David Raser, the 915th CWB Operations Officer (S-3), the battalion has (17-series Military Occupational Specialty) cyber and EW officers, NCOs, and enlisted Soldiers, as well as IO, Signal, Psychological Operations and SIGINT personnel. And much like other Army battalions, there are support personnel, such as administrative and supply specialists, in the headquarters.

Soldiers interested in serving in the 915th CWB should contact their organization career counselors or branch managers.

For a fact sheet on the battalion, go to https://go.usa.gov/xpfEg.

HOHENFELS, Germany – *Expeditionary Cyber Operators from Expeditionary Cyber Team 1, 915th Cyber Warfare Battalion, pose before moving out on a mission on September 21 at the Joint Multinational Readiness Center.*

Risk and Disciplined Initiative

By Capt. Tamara Rainford, company commander, Headquarters & Headquarters Company, 781st MI BN (Cyber)

Imagine a war controlled by ones and zeros rather than bombs and bullets. A war fought in assumed silence, and resulting in an unforeseen tangible aftermath. The phenomenon of the hybrid threat is the driving force of modern warfare and exists in many forms. Cyber warfare is a dimension of the hybrid threat where in which an aggressor uses technology to undermine and gain the advantage over an opponent. These sophisticated and flexible adversaries challenge our leaders to operate effectively in an ambiguous and dynamic environment that requires constant adaptation. As such, the ability of leaders and subordinates to envision, conceptualize and make decisions within their commander's intent is crucial to winning battles in today's modern combat atmosphere. Due to the ubiquitous essence of cyber warfare, it is important to explore the nature of daily military operation requirements and decision making both at the point of action and in the context of the interrelated principles of mission command.

The nature of military operations is characterized by constant, mutual adjustments of all involved personnel. A commander controls the operations process, the continuous cycle to lead, understand, visualize, describe, direct and assess pertinent objectives. Supporting staff and commanders at all levels have the inherit responsibility to lawfully make decisions and direct actions for mission accomplishment. The principles of mission command were developed over time and provide a framework from which leaders can work to achieve the desired end state. Exercising discipline initiative and accepting prudent risk are two of the interdependent principles of mission command, which offers structure to leaders combating the hybrid threat in austere environments.

Modern warfare requires leaders to recognize and enable the capabilities and limitations of their subordinate leaders, Soldiers and equipment. Leaders must develop timely decisions as it relates to the daily military operational environment within the context of intent. Providing trusted personnel with the liberty to take on more responsibilities in the absence of orders creates opportunities to resolve unexpected complications associated with a specific situation or operation. Additionally, subordinates who demonstrate discipline initiative, as well as innovative and novel methods of completing tasks contribute to the achievement of mission success. As a result, allowing freedom of action to alter existing plans within the commander's intent introduces new techniques and tactics practices (TTPs).

Balancing risk with opportunity is a significant yet daunting task for any commander. Due to the marginal degree of unpredictability innate to warfare, all military operations are inherently risky. This principle of mission command is important because assessing and adjusting risks create chance and alter previous estimations of success. Therefore, it is necessary for commanders at all levels to evaluate risk assessments frequently to determine risks and apply solutions to manage and mitigate them. Prudent and sensible risk taking is essential to overcome the challenges leaders and subordinates encounter during daily military operations.

Our enemies across the globe cultivate new strategies to inflict confusion and chaos as the world becomes increasingly interconnected. Army leaders must practice and emphasize the principles of mission command at multiple echelons to maximize mission success. The mission command model and its principles are critical for the cyber warfare landscape as cyberspace operations ranges throughout all physical domains. At the lowest level, cyber warriors are charged with executing operations by balancing mission requirements, risk and initiative in harsh environments. The mission command principles as a collective approach creates agile and adaptive forces consequently resulting in active leadership.

General Heinz Guderian and Mission Command

By Capt. Joseph Dooley, company commander, A Company, 781st Military Intelligence Battalion (Cyber)

The U.S. Army's command and control doctrine is simple: empower subordinate decision-making, decentralize execution, and use mission orders to enable disciplined initiative in accomplishment of the commander's intent. As any leader will admit, the practice of this mission command philosophy takes personal courage. There is no shortage of examples of this in the long history of our profession. One such thought leader and innovator from the second world war, General Heinz Wilhelm Guderian, is the grandfather of Blitzkrieg tactics and the German armored corps.

Leaders recognized their devastating power, but Guderian's ideas were met with overwhelming resistance by his command. While his leadership saw the armored forces as a supporting element, Guderian knew these capabilities were superior to infantry. His radical notion was to concentrate armored forces on key terrain vice the accepted norm of battleground decentralization. Guderian correctly paired capabilities to relevant targets.

The exercise of disciplined initiative of commander's intent is a critical component of successful mission command. Leaders at the point of action must assess the situation, make timely decisions in response to changes in operational environments, and take actions aligned with achieving desired end state of commander's intent. Guderian exercised disciplined initiative through innovative battle tactics and capabilities, which rejected the norm.

Guderian was heavily influenced by Napoleon Bonaparte's high operational tempo via rapid communication of intentions and rationale. Junior leaders' initiative resulted in a tempo that left adversaries bewildered. If order execution is rendered impossible, leaders must to act in line with intention. Mistakes are preferable to hesitancy to enable decisive action. Guderian understood commander's intent of German victory and acted accordingly.

This is echoed by General Stephen Townsend, the commander of U.S. Africa Command since July, and previously the commanding general of U.S. Army Training and Doctrine Command, when he said to "have the discipline to follow your orders until you realize they're not going to work or they don't pertain anymore. Come up with a plan that will work and have the guts enough to do it."

Making reasonable estimates and intentionally accepting prudent risk are fundamental to mission command. Leaders must continually conduct risk assessments to determine risks and implement solutions to mitigate them. Leaders cannot eliminate all risks so accepting prudent risk may be required.

Guderian accepted the risk by pressing ahead through opposition to create a modern force remarkably effective against the Allies during WW II. Guderian knew early German tanks had unsatisfactory specifications and ordered improvements to compensate for enemy improvements. Guderian took aggressive action and accepted the risk of untested capabilities. In addition, earned the trust of his subordinate leaders to take ownership of the risks themselves.

Parallels between German armored corps and U.S. Cyber Mission Force are poignant. Many of the challenges Guderian faced are similar to the establishment of U.S. Cyber Command and challenges mission and team leads face today. Just as with Guderian's armored corps, there are competing ideas within the cyber community on training, employment, scale, scope, and capabilities development. Leaders must accept risk and take disciplined initiative in pursuit of mission accomplishment in order to achieve institutional change and mission accomplishment.

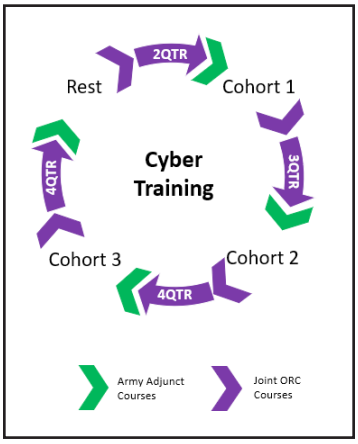
Read the AvengerCon IV story on page 23

Changing the Culture of Cyber Training

By Capt. Lauren Feifer, company commander, B Company, 781st Military Intelligence Battalion (Cyber)

Cyberspace is a uniquely challenging operational domain, necessitating persistent engagement with our adversaries. These adversaries are additionally unique in their ability to executive a wide spectrum of operations with near-peer capabilities. As the military requirement for a formalized cyber force within this domain rapidly arose, the intrinsic relationship between U.S. Cyber Command and the National Security Agency undeniably enabled the CMF's (Cyber Mission Force) FOC (Full Operational Capability) status. Notwithstanding this significance, USCYBERCOM's adaptation of the NSA's experience, processes, and tradecraft have fostered a risk adverse operational force with little maneuver space for exercising disciplined initiative at lower echelons. The relationship between USCYBERCOM and the NSA is a palpable argument defending leadership challenges surrounding the employment of the Army's Mission Command principles. Predicting the inevitable, unscheduled, and highly political split between the two organizations, what can Leaders in our formations do today?

General Paul Nakasone, who leads both USCYBERCOM and NSA, overarching intent for each Service is to man, train, and equip the CMF. A connective tissue that exists between both USCYBERCOM and the NSA is training. The current J7 (the staff section responsible for training) pipeline embodies a reliance on NSA systems and databases, that is currently unavoidable. This noticeable and intentional imbalance cannot shift without a USCYBERCOM independent infrastructure, architecture, and intelligence support systems. Given these constraints, the Army is building towards Title 10 focused training, deliberate utilization of adjunct faculty, and recently approved the implementation of JQR (Joint Qualification Requirements) based training certification. A method we can directly exercise disciplined initiative while increasing readiness is through a methodological shift in the acquisition of NSA required training.



Deviating from the current and highly fluctuating requirements-based training plan, an alternate method of delivery exercising disciplined initiative is the cohort model. The CMF previously utilized and revoked this process due to the large number of empty training seats. MARFORCYBER (U.S. Marine Corps Forces Cyberspace Command) executed a cohort delivery this year, with a second planned by AFCYBER (Air Forces Cyber) in January 2020. This methodology allows for a predictable training schedule where Army adjunct offerings fulfill additional requirements, similar to the TRADOC-like TRAP (Training Resource Arbitration Panel) process. The previous cohort delivery of NCS (National Cryptologic School) courses was arguably disproportional to the CMF requirements. The vast number of offerings allowed personnel to "wait for the next class", thus creating a significant waste in both cost and time. The proposed model includes a scaled approach of quarterly based joint NCS pipeline classes, Army augmented adjunct courses, and chronological delivery of senior work-role progression training (i.e. exploitation analyst (EA) and interactive on-net (ION) operators specific ORC courses).

Limited number of offerings and Army only adjunct courses are key to the success of this model. Three proposed cohorts within a fiscal year allows for predictable Solider and Civilian training schedules (for both students and adjunct faculty instructors),

Continued on page 44

Discipline, an essential element of cyber operations

By Capt. Stephen Hart, company commander, C Company, 781st Military Intelligence Battalion (Cyber)

Discipline, an essential element of cyber operations, enables commanders to take prudent risk and trust their Soldiers initiative. However, discipline is not an innate characteristic and leaders must develop and hone discipline in Soldiers. When the Soldiers and Civilians of the 780th Military Intelligence (MI) Brigade (Cyber) continuously perform mission they have limited time to develop discipline through training and exercises. Concurrently, the Cyber Mission Force (CMF) uses extensive classroom instruction to train cyber warriors, but leaves out experiential training. A disciplined cyber Soldier must have the maturity to deliberately plan and execute in cooperation with many interdisciplinary teammates. Allowing Soldiers to collectively demonstrate discipline on keyboard and improve their tradecraft through situational training exercises (STX) would help improve their motivation and mission outcomes.

Cyber Soldiers endure long training periods before they can function as a good teammate. As they grow, they should have more opportunities in low risk environments to function on their teams in both training and operational roles. Those opportunities will allow assessment of their discipline while feeding the desire that brought them into the CMF.

Continuously pursuing mission can only allow limited growth. Certain situations must be practiced so that when seen in real life, Soldiers handle them appropriately. The Army values tough realistic training to prepare Soldiers for battle without placing them in unnecessary danger. Tough realistic training in cyberspace requires spending time away from the ever growing live mission to learn from new experiences.

Opportunities to fail gracefully allow Soldiers to build confidence safely without harming mission and provides opportunities for leaders to assess their Soldier's discipline. When a Soldier fails in an exercise it can be transformed into a learning opportunity instead of risking millions of dollars of development cost. However, exercises are only effective if they replicate some aspect of what Soldiers expect to see in combat.

Opportunities that allow Soldiers to fail gracefully can be difficult on an active mission, so the Army must deliver robust threat emulation for Soldiers to train on. This requirement becomes more obvious when one considers that the split between defensive and offensive cyber operations in training is arbitrary. One is merely the trainer for the other. The lacking piece is sophisticated emulation of the adversary.

Soldiers learn risk taking when they build the ability to estimate their abilities in context to their surroundings. Prudent risk takers know themselves and their environment well. Further, leaders cannot grow their own knowledge without exercising risk making decisions. A STX allows a small unit to develop an understanding of itself and its internal team dynamics. In an STX there exist two levels of risk to train on. First there is the exercise risk. The exercise risk involves keeping participants safe during execution. Second there is game play risk as defined by the range of options the participants can execute. For example, how will the Soldiers navigate terrain to avoid the enemy or place the platoon's weapons squad for maximum lethality. Those small decisions each carry decision making that leaders must balance.

In wars where fear dominates Soldiers ability to fight, discipline ensures Soldiers are ready and fight in the face of grave danger. Cyber warfare lacks the physical danger that caused the Greeks and Romans to organize into highly disciplined phalanxes. Instead, the subtler danger of misusing tools or inadvertently identifying presence to the adversary dominate the risks of cyber warfare. The same discipline to prepare, stay alert, and fight until the mission is complete is still necessary, but takes on a mental instead of physical tone. STX's help build mental toughness that will improve the results of cyber operations.

Continued on page 44

Scrum: How CSD Manages Risk and Achieves Disciplined Initiative

By Capt. Justin Lanahan, company commander, D Company (CSD), 781st Military Intelligence Battalion (Cyber)

The Cyber Solutions Development (CSD) Detachment develops timely, innovative, and operationally relevant capabilities in order to enable cyberspace operations. This process is inherently risky because software engineering requires making investments and decisions of which the consequences may not be known until after a product is already delivered. Additionally, the complex nature of Computer Network Operations results in many projects that may never actually see success, but never-the-less still must be fully explored and exhausted. These facts coupled with bugs introduced by human error and sometimes long production times means cyber capability development is especially uncertain.

CSD manages these problems by aligning the tenets of agile to the six principles of mission command. Agile is a process framework leveraged by the tech industry for addressing complex problems, while also being flexible and able to quickly react to change. The process is intended for use by small teams that integrate all product stakeholders from the start to create shared ownership. CSD uses agile to foster self-organizing, cross-functional development crews that have mutual trust and a shared understanding as enabled by the commander's intent.

The effect of agile is that developers can exercise disciplined initiative to quickly react to changing requirements and seize opportunities. These opportunities come from the freedom of movement allowed at the lowest level in the absence of orders and take the form of integrating new research and technological innovations, partnering with joint organizations on hard problems, and constantly being on the hunt for any manner of overcoming obstacles.

Just as important to minimizing risk is also accepting prudent risk. Developers in the CSD do this daily through experimentation within the constructs of Developmental Test & Evaluation. Unit tests are built according to customer requirements that serve as a defined end state. Developers are then given broad means of achieving these goals which open up entirely new sets of opportunities as TTP's evolve.

The guiding principles of agile are further refined by the scrum methodology, where small, iterative development is emphasized. Scrum allows section and crew leads to control the tempo through time-boxed sprint cycles, which are short 2-3 week periods of development in between periods of planning, testing, and customer reviews. Such tempo enables CSD to minimize interruptions while sustaining readiness by mapping sprints to the ARFORGEN model.

Scrum is the core of how CSD minimizes risk by embracing a "fail fast, fail often" philosophy to ensure continual delivery and improvement. Empirical process control drives these mechanisms with transparency, inspection through feedback, and adaptation via retrospection and constant risk identification during sprint standups. The artifacts of this process are distinctly measurable according to backlog management, product increments, testing code coverage, development velocity, and burn down charts spanning development cycles to name a few. Collectively, these metrics inform future resourcing and further help manage risk.

Together, agile and scrum encourage a level of creativity and innovation that results in the highest quality capabilities with a greater impact on mission success. Scrum is how the CSD trains and scrum is how the CSD fights to lead the way in delivering world-class cyber solutions.

Trunk or Treat & Holiday photos

Courtesy Photos

GROVETOWN, Ga. *– The Headquarters & Headquarters Company, 782nd Military Intelligence Battalion (Cyber) hosted their Trunk or Treat at Steed Dairy Farm – Little Annie is Penny Sanders, Lt. Col. Wayne Sanders was Ferris Bueller, Maj. Brian Lebiednik was a wizard, the pirates are Capt. Maribel Brown, HHC company commander, 1st Sgt. Lorne Barber, and Capt. Brown's husband.*

FORT GORDON, Ga. *– Lt. Col. Wayne Sanders, commander of the 782nd MI Bn., at the HHC Holiday Party on November 22 in the Reserve Center.*

AUGUSTA, Ga. *– The 782nd MI Bn. also hosted a Halloween Fun Run on Oct. 31 at the Savannah River Rapids Trail.*

Disciplined Initiative: An American Advantage

By Capt. Maribel Brown, company commander, Headquarters & Headquarters Company, 782nd MI BN (Cyber)

As I walked into the expansive motor pool on a sunny morning in an Eastern European nation, my inner leader sensed something was wrong. As I looked around at the rows of Soviet-era vehicles sitting dormant, I took a moment to appreciate the opportunity I had been given in coming to visit this country as an ambassador from my unit. I looked at the faces of that country's service men and women as they sat around in small circles, smoking cigarettes, and talking quietly amongst themselves. That's when what was wrong hit me. None of them were working!

My escort introduced me to the motor pool NCO and I asked him what they were working on today. In heavily accented English, which belied his strong grasp of our language, he told me they were waiting on their Captain to come back from his meeting. "We do not do anything without receiving orders," he explained to me. "The Captain is meeting with the Major, and when he gets back he will tell us what vehicles we need to work on and what we are doing today. He will explain it to the Lieutenants, they will come tell us, and we will get our soldiers together to start working on it." I was stunned. I was a First Lieutenant at the time serving as a platoon leader. I knew even though I was TDY that week, back in Italy my Paratroopers were executing battle rhythm tasks and leaning forward to prepare for our upcoming field exercise. I knew without having to ask that all of our vehicles had received maintenance on Monday. I asked the motor pool NCO, "Doesn't that process just slow down productivity? What happens if the Major or Captain isn't here?" He merely shrugged. "Then nothing gets done. This is always how we have done things here," he quipped matter-of-factly. I was astonished a 21st century army still had a rigid, centralized command structure that immobilized junior leaders and made them afraid to act in the absence of orders.

The concept of exercising disciplined initiative is one of the six tenets of mission command. While mission command is not an exclusively American concept, having deep roots in Prussian and Napoleonic times, it is a concept the American army has learned to hone and execute elegantly. At one point during my first assignment as an officer, the Brigade had Soldiers spread across 16 different countries in four time zones executing countless different missions. The commanders of the unit underwrote the prudent risk of sometimes having a Second Lieutenant or a Staff Sergeant as the highest ranking person in a country, and trusted they would exercise the disciplined initiative to meet the Commander's intent with minimal communication back to headquarters. As an American unit operating in Europe, we understood something some of our allies did not - to remove disciplined initiative is paralyzing. By removing the opportunity for leaders to accomplish tasks within the Commander's intent, the unit becomes stagnant, and junior and mid-level leaders lose an opportunity to develop. In the American army, and especially in the cyber world, the extreme decentralized nature of what we do requires that we exercise disciplined initiative under the larger umbrella of mission command. The focus on this phrase is the "disciplined" portion, as initiative is tempered by the prudent risk mission commanders and other leaders exercise during operations.

Clausewitz wrote, "War is a continuation of politics by other means." Likewise, cyber operations are an extension of other aspects of war, usually during the period short of conflict. The missions the 780th MI Brigade completes are just as complex, if not more so, as those of any infantry or artillery brigade. Our firing platforms are different, but the end state is the same and our application of leadership principles must also be the same. Leaders in the Cyber branch must continue to exercise disciplined initiative as they navigate the complicated cyber terrain and underwrite the prudent risk involved. Otherwise, we will become paralyzed and unable to face ever-evolving adversaries and challenges.

Disciplined Initiative and Risk – Where to draw the line?

By Capt. Ty Clayton, company commander, A Company, 782nd Military Intelligence Battalion (Cyber)

As the newest battle space, Cyber is evolving and along with that evolution comes growing pains. These irritants appear in the form of restrictive policy, "unwritten rules" that have yet to be documented properly, and leaders who are unwilling to delegate any legitimate level of risk. In other branches junior leaders are allowed the freedom of maneuver when planning and executing operations by utilizing disciplined initiative and prudent risk. We as a cyber force need to continue to strive for this same model. The more we allow our leaders at lower echelons, primarily combat or national mission team, to exercise disciplined initiative and prudent risk the more success we will in turn have as a force. The current approval levels for basic level operations in the cyber domain require General Officers to sign off on, who may lack an understanding or appreciation of the technical details of the mission.

Take a look at how the Army is able to engage enemies in more traditional battle spaces such as land or sea. The approval authorities to engage are at a much lower level depending on the nature of the target, and taking into account any civilians or civilian infrastructure. The typical rules of engagement are ingrained in every Soldier prior to deployment so that they know exactly what they can and cannot do in the absence of orders. This allows our junior leaders in these fields much more autonomy to exercise disciplined initiative and acceptance of risk in the tactical environment. These crucial elements of mission command are what enable our forces to excel against our adversaries on a consistent basis. Trust is built through enabling these junior leaders to execute mission supporting the commander's intent. While engagements in these domains tend to be of the tactical variety, they still have potential strategic level impact similar to their cyber counterparts. However once the targets are vetted and validated through the joint targeting cycle the "go-ahead" is not held at such a high level by comparison.

The very nature of the Cyber field is constantly changing, as our adversaries' adapt their utilization of the Internet against us. Our leaders at the team level and below are actively engaged and have that tactical level knowledge necessary to execute operations. However, the current requirements laden on teams to initiate these operations significantly delays the execution and potentially limits the impact teams are able to provide. These restrictions of not delegating the acceptance of risk at higher echelons prevent teams from acting in a more real time manner. Due to the expense of cyber tools and sensitivity of individual techniques risk acceptance has yet to be delegated down to an actionable level. While this is understandable to a degree, these can be mitigated by empowering team leads and more senior operators. Ensuring that you have subject matter experts sets you up for success regardless of the domain. Oftentimes the process to get certain operations approved in cyber take upwards of three to four months from the time a target is identified until it is ultimately actionable. In order to remain an effective force leadership at these upper echelons needs to adapt a taste for delegating down this risk acceptance. As cyber continues to grow and evolve these are some of the necessary steps to ensure long-term viability, and our usefulness to the ground force commanders.

GROVETOWN, Ga. – *782nd MI Battalion hosted a Fall Festival full of trunk or treat, chili cook-off, hayrides, and plenty of activities for the kids at the Steeds Dairy Farm on October 23. (Courtesy photo)*

Don't stifle the innovation, it just might save lives

By Capt. K. Lee Shelton, company commander, B Company, 782nd Military Intelligence Battalion (Cyber)

During World War II my grandfather received a reprimand and a commendation for the same action. His Marine Company was pinned down by Japanese Zero airplanes that were strafing him and his comrades with machine gun fire on a battle torn island during the south pacific campaign. My grandfather, being the scout sniper of his platoon, raised his rifle in an attempt to shoot down the plane. His commander ordered him not to engage the airplane and give away their position. Ignoring the order, Lance Corporal William McAvoy shot at the plane, hit the plane and struck something critical, which then caused the plane to crash. Other planes in the formation upon seeing this flew higher and were not able to effectively engage the ground troops, resulting in less American casualties.

I have seen recent actions in the cyber force where junior cyber leaders were initially reprimanded and subsequently rewarded for the same action in cyber space. In cyberspace we are handcuffed by many rules and regulations that stifle innovation and the exercise of disciplined initiative. Many successful leaders in Army history have learned to be agile and adaptive by accepting prudent risk, executing their mission with violence of action, and learning from their failures as well as their successes. We must get to a point in the cyber force where we trust our lower level leaders to exercise disciplined initiative in order to become a more lethal force. We cannot grow until higher headquarters' are willing to accept some prudent risk, and underwrite honest failures of aggressive subordinate leaders.

Mission Commanders Are Not Trusted to Exercise Disciplined Initiative

Two years ago I attended the mission commander course. During the first class, the instructor asked, "What is a mission commander?" The resounding response was, "The fall guy!!" Mission commanders in the current construct are held responsible for everything that happens during an operation, but yet they do not have the decision-making authority to go along with this responsibility. They cannot make their own risk decisions. Aside from causing confusion and delay during operations, this undercuts the mission commander's authority. Thus, mission commanders are not allowed to exercise disciplined initiative.

Shortly after becoming certified I was running an operation and suggested we use an open source technique. "We can't do that, sir," said the operator. "Why not?" I asked. "Because it is not approved, Sir". So I asked, "Will it work?" "Oh yeah Sir, that will definitely work. But we will have to call CTOC, we will have to have the WTD review it…" As the operator and EA went on telling me about all the levels of approval I had to go through, I realized there was no way it was going to happen during the op. I felt as if all I was doing was riding along and taking notes. I did not feel empowered to make risk decisions commensurate to a captain's rank at all.

On another occasion, a mission commander assumed risk on an operation and made a decision that was critical to mission success, without notifying higher headquarters. The mission was in fact a success. The collateral damage was minimal and mitigated. But the mission commander was de-certified, and taken off the ops rotation for a short period in order for him to be re-trained. Soon afterward, he was awarded a medal for his actions that were critical to mission success.

The danger here is not that we have loose-cannon MC's running ops. The real danger is that we are stifling creativity, mental agility, and adaptive thinking. If we treat high performers badly, they go into "CYA" mode and now they become mediocre performers that are risk averse. Also, if we do not hold low performers accountable, or if we treat them well instead, they assume the standard is low and never achieve a higher level. What we end up with is a force that is mediocre and complacent across the board. Unwilling to take calculated risk, and

Continued on page 45

Disciplined Initiative and Risk

By Capt. George R. Thursby, company commander, C Company, 782nd Military Intelligence Battalion (Cyber)

Officer, or Enlisted, those are the two choices to choose when entering the Army. When you sign the dotted line, you wittingly or unwittingly, sign into a profession. For some, understanding what that profession is, can take years to understand. The ones who do, become an NCO, Warrant Officer, or continue to stay as an Officer. They put in their time and effort, but why? Some of the attributes defined in ADP 6-22 Army Leadership could explain it: Confidence, Resilience, Innovation, Discipline, or Sound Judgment. Perhaps though, there are deeper feelings and meaning; the pride of becoming a professional in the Army profession. Disciplined initiative and calculating risk are two important factors becoming a professional in the Army, but it requires time and dedication like all other crafts.

Elon Musk said "You get paid in direct proportion to the difficulty of problems you solve". For the proverbial "us" that can directly relate to how we all get promoted at some point in our careers; the higher the rank, the more responsibility. However, more responsibility does not equate necessarily to problem solving and good decision making, two outcomes of calculating risk and taking disciplined initiative. There are certain levels of understanding when making decisions. As mentioned by a clinical psychologist from the University of Ohio, Dr. Ellen Peters, she determined it is how people learned to process information, which ultimately determines the choices they make.

For example, if someone was raised by someone to think avoidance throughout their life, they will have a higher chance processing information on how to avoid uncomfortable situations, therefore more risk avoidant than taking risks. The reciprocal would be, if someone were raised where there were no one to tell them what was risky behavior or not, they'd have a higher chance of taking risks. However, the Army doesn't get to choose those who are comfortable taking risks versus who are not, and which is best for what scenario for that matter. The good news is though, the psychology community determined that calculating risk is a learned behavior, and the Army through its professional programs can teach and mentor those how.

Part of joining a professional organization whether recognizing it or not, is mentorship and guidance go second hand. Those who have achieved the highest ranks in the military will tell you that have had mentors throughout their career. For those who are the youngest in their careers, a mentor is paramount for success. Taking the initiative as a young soldier to find that mentor which will help you and reciprocally, taking the disciplined initiative as the mentor to teach, and coach that new Soldier is paramount for the success of the organization. For the Cyber Branch, it is of the utmost importance to continue the professional model the Army has established for teaching and mentoring among transferring years of technical and operational experience to those, but professional lessons such as how to calculate risk, and understand disciplined initiative. As we know, the cyber domain is as nebulous as if not more nebulous as world politics. Our junior and senior leaders must approach the domain with the mature professional understanding, and those who take pride in their profession will drive our organization with disciplined initiative and calculated risk.

Leadership for Low-complexity Missions

By 1st Lt. Joshua B. Fielder, company commander, D Company, 782nd Military Intelligence Battalion (Cyber)

Is time to reconsider the requirements for tactical leaders in the offensive house of U.S. Cyber Command. The authority and responsibility of tactical leadership for a cyber tasking order has been bestowed upon a Mission Commander (MC) since the establishment of the workrole in 2014. The MC designation has traditionally been reserved for commissioned and warrant officers. These individuals are qualified and postured for conducting traditional offensive cyber operations of high, technical complexity. Yet with this level of expertise, should an MC be responsible for executing all cyber tasking orders regardless of the mission's technical complexity? USCYBERCOM is testing that question after having relaxed the rank requirement (on a trial-basis) for conducting operations of lower technical complexity with the implementation of the new Mission Lead (ML) workrole - available to NCOs.

NCOs are exercising disciplined initiative in defining the ML training requirements based on the foundations of the MC workrole. So what are Mission Commanders responsible for? Executing the Commander's taskings by gaining an understanding for the underlying purpose and intent for the mission. "MCs are chosen based on their situational awareness of the fight and/or preponderance of mission capability. MCs should embody a command mindset. An MC must be ready to delegate, make tough decisions and act decisively. MCs should possess a solid foundation of cyber warfare operations, the capabilities to be employed and associated TTP." (USCCI 3300-06) MCs have to be organized, prepared, and able to accomplish a plethora of responsibilities. As this workrole is tested and defined, the qualifications for a Mission Lead may be very similar to that of a MC, but without the requisite training requirements. So how does the ML differ from an MC?

This new leadership role necessitates lighter, albeit appropriate, training requirements. The ML is focused on leadership, administration, and enforcement of procedures; understanding and applying technical cyber capabilities is no longer their top priority. More sophisticated mission sets will remain under the leadership of the traditional MC. And yet the lack of complexity presents its own challenges: the leader needs to keep their team engaged through potentially routine and straightforward phases of a mission. That is not to say they will not be challenged as a tactical leader; MLs must also exercise disciplined initiative by making final decisions within the constraints of the operation. To ensure the success of an ML, the commander should be on-call, verify the teams proficiency through periodic training/assessment, weekly activity reports, and open dialogue.

The ability to delegate taskings to a Mission Lead is determined by the higher headquarters, but could possibly be based on the subjective determination of the current leadership structures. Therefore, MCs as well as Team Leads may one day have the authority to delegate the leadership of specific operations to a qualified NCO. Delegation would enable MCs to focus their efforts on the rigors of their complex missions while giving autonomy to the ML and their team members. Whoever is responsible for assigning the tasking to the ML assumes a degree of prudent risk in allowing the ML to own and operate their mission. It is taking a risk in territory that is not unfamiliar to the MCs, therefore the transition should be fairly simple with the passing of the lessons learned. Ultimately, the Commander is responsible for giving their vote of confidence and ensuring that MLs are trained to standard; at present those standards are still being assessed and codified. This passing-of-the-torch from an MC to an ML is a display of confidence and a wonderful opportunity for the enlisted soldiers of the Cyber Mission Force.

Whose risk is it anyway?

By Capt. Joseph Lucas, company commander, E Company, 782nd Military Intelligence Battalion (Cyber)

Soldiers and Civilians reading this article administratively belong to the 780th Military Intelligence Brigade and Intelligence and Security Command, but they work for a variety of operational headquarters. Each Soldier or Civilian is therefore at the junction between two distinct chains of command. DA PAM 358-30 (Safety Risk Management) states that "risk management provides Commanders with the ability to balance risk levels with other desired outcomes." However, the disunity of command implicitly creates competing desired outcomes, perceived impact to mission, and therefore hazard identification and mitigation strategies. This disunity often forces individuals to balance risks and priorities between their headquarters, as opposed to asking a Commander to accept that risk. In cases where one of the Commanders does choose to accept risk, he or she must consider the desired outcomes and risks to the complementary Commander. Here is a case study.

PFC Snuffy fails their second record APFT and is also re-enrolled in ABCP within one year of exiting the program previously. Most Army units would separate a Soldier for either of these offenses. However, AR 350-1 does give Commanders the discretion to bar a Soldier from continued service for either infraction. Most leaders generally accept that fitness standards are an important ingredient to maintenance of good order and discipline. It is therefore a hazard, a threat to the unit's cohesion, to retain a Soldier who shows a continual inability to meet these standards. Knowing this, the Company Commander, CPT Smith decides to simply bar the Soldier from reenlistment instead of initiating either available chapter option. Why?

CPT Smith may accept this risk not out of thought for his own Command, flowing to his Company from the 782d Military Intelligence Battalion, the 780th Military Intelligence Brigade, and Intelligence and Security Command. Instead, his thought could be for the operational effectiveness of the operational headquarters. This Soldier could be integral to our conduct of offensive cyber operations. Not the Company's operations, ARCYBER's. Was this risk prudent for the Company? No. Was it prudent for the operational headquarters? Yes.

DA PAM 358-30 (Safety Risk Management) continues to state that "accepting risk is a serious matter; therefore, the appropriate level of Army leadership must weigh the increased danger to the mission, [etc] against the operational requirement that necessitated acceptance of a significant level of risk." However, in this case, the Cyber Mission Force separated the "operational requirement" and the risk accepting authority.

There are several reasons that this administrative and operational structure exists, but it is contrary to Risk Management doctrine. Ironically, that itself is a risk that some commander accepted. Based on these chains of command, I don't know who.

1st place Trunk...

1st place costume.

FORT GEORGE G. MEADE, Md. *– Headquarters and Headquarters Company, 780th Military Intelligence Brigade (Cyber), and E Company, 782nd MI Battalion hosted a Trunk or Treat on October 29. (U.S. Army photos)*

An Army "hacker con" goes big: The return of

By Sean Gallagher, IT and National Security Editor, ars Technica

***COLUMBIA, Md.** – AvengerCon is a free hacker event held every fall to benefit the hackers of the U.S. Cyber Command community, and is supported by the U.S. Army 780th Military Intelligence Brigade (Cyber). This year's event was hosted at the DreamPort facility in Columbia, Maryland on October 17 and 18. (U.S. Army photos)*

COLUMBIA, Md.—In a business park that plays home to a number of tech and cybersecurity firms situated strategically between Washington, DC, and Baltimore, there's a two-story building that looks externally like many other office buildings, remarkable this day only for the food trucks in the parking lot and the stream of people in camouflage swarming in and out. The building, called DreamPort, is a collaboration facility leased by US Cyber Command—and on October 18, it was the location of AvengerCon IV, the latest incarnation of a soldier-led cybersecurity training event that takes the shape of a community hacking conference.

The event also offered USCYBERCOM a chance to show off DreamPort—and a chance for me to meet with David Luber, the Executive Director of USCYBERCOM.

"AvengerCon is an event that is attracting the very best talent both from our DoD participants and also from some of the folks that are working with us outside of the DoD," Luber said. "When you bring those very best cyber experts together, they get to learn, test out new ideas, and work in an environment that is hosted by and for DoD cyber operations community experts. They're working in a community of peers—they get to learn together, they get to fail together. And what we've seen from previous activities with AvengerCon is that it's an exhilarating, fun environment for them to work in, and they learn a ton while they're here. And the private sector benefits because as AvengerCon shows, we're all working on some of the same cyber challenges together."

AvengerCon is an effort to bring the learning environment provided by security conferences such as DEFCON to a military and government community that wouldn't otherwise be available because of cost and bureaucratic complexity. Originally a training event organized by the 781st Military Intelligence Battalion at Fort Meade involving about 100 soldiers, AvengerCon has grown to 600 attendees and has gained the backing of Army Cyber Command and USCYBERCOM.

"My job, in part, is trying to figure out how to properly train soldiers in a field that doesn't have decades of standard operating procedures and clear paths for training to get to success," Capt. Joseph Dooley, an organizer of AvengerCon, told Ars. He said that this type of event offered "a unique opportunity for soldiers to individually be in a more unstructured environment where they can set their own agenda"—where they can pick things that they're interested in or feel they need training in without the usual constraints of formal Army training.

The event "complements efforts in regular unit

AvengerCon

training," Dooley explained. "And it gives [attendees] the chance to collaborate with subject-matter experts [and] share and compare tradecraft, best practices, and ideas. This is a very good way to boost our other conventional training."

Sgt. 1st Class Craig Seiler, another member of the AvengerCon organizing committee, said that bringing together people from across the cyber operations community in government provided a boost to the learning opportunities. "What we've found is mixing all these different types of people—developers, people doing operations—they all do great things separately, but when they get together later on, they say, 'Hey, I really learned something from that analyst or that developer that I've picked up to bring to my current job.'"

I attended last year's AvengerCon, held on Fort Meade, at the invitation of the unit organizing the event, the 780th Military Intelligence Brigade (Cyber). While AvengerCon III was clearly a success, this year's expanded event puts AvengerCon on the scale of well-established regional security conferences. The keynote speaker was security researcher Daniel Cuthbert, who is Global Head of Cyber Security Research for Grupo Santander and co-author of the original Open Web Application Security Project (OWASP) Testing Guide and the OWASP Application Security Verification Standard. He spoke largely on the issues surrounding information-sharing and collaboration in the cybersecurity realm.

Holding a "con" on a military post (and at Fort Meade in particular) can pose some logistical challenges—such as getting people cleared and onto the base itself, and limited space to stage the event. Fortunately, the success of AvengerCon drew the attention of US Cyber Command, and the organizers were offered the use of DreamPort for the event's next iteration.

AvengerCon fits neatly into DreamPort's mission to foster collaboration between US Cyber Command, the rest of the Department of Defense and intelligence community, and industry.

"We opened the facility here in Columbia, Maryland, back in the fall of 2018," Luber said, "created under a partnership intermediary agreement between US Cyber Command and the Maryland Innovation and Security Institute [MISI]. We've hosted over 14,000 visitors in this 40,000-square-foot facility, and in June of 2019, MISI signed an expansion lease to double the size of DreamPort by the end of 2020. So, we're really happy about the partnership that we've had so far."

Companies and individuals can come into the unclassified facility to demonstrate capabilities during

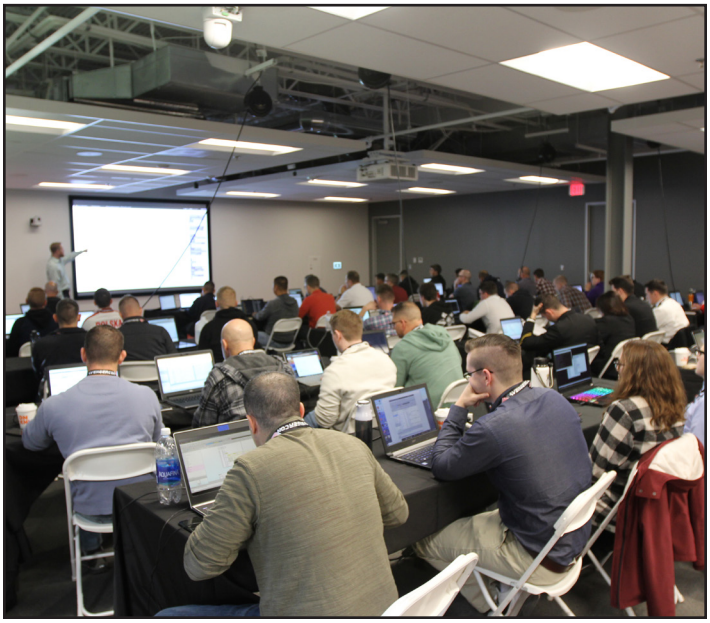
Continued on page 43

***COLUMBIA, Md.** – Since its inception in 2016, the principles of AvengerCon have been to promote the hacker culture from the grassroots level of U.S. Cyber Command, and to develop and grow junior members of the organization by providing a platform for learning, contributing, and mentoring. This year's event is hosted at the DreamPort facility in Columbia, Maryland on October 17 and 18 and the keynote speaker was Daniel Cuthbert.*

COLUMBIA, Md. *– AvengerCon is a free hacker event held every fall to benefit the hackers of the U.S. Cyber Command community, and is supported by the 780th Military Intelligence Brigade (Cyber). This year's event was hosted at the DreamPort facility in Columbia and on Oct. 17 and 18 and the keynote speaker was Daniel Cuthbert. Since its inception in 2016, the principles of AvengerCon have been to promote the hacker culture from the grassroots level of USCYBERCOM, and to develop and grow junior members of the organization by providing a platform for learning, contributing, and mentoring. (U.S. Army photos)*


RF VILLAGE


Detection & Analysis
Containment Eradication & Recovery
Post-Incident Activity
NIST SP800-61
splunk




GRIMM
EARTH TREKS

How Disciplined Initiative is Building Our Expeditionary Cyber Force

By Capt. Allyson I. Hauptman, company commander, Headquarters & Headquarters Company, 915 CWB

In an ideal world, military units are composed of a carefully determined mix of MOS's, ranks, and skill identifiers. This mix is the product of multiple working groups, years of experience, and periods of trial and error. It is a formula reliant on time and a large pool of talent from which to draw upon. The reality in which the Army is building its expeditionary cyber force, the 915 Cyber Warfare Battalion (CWB), is far from ideal. Army leadership determined that the risk of waiting to standup the battalion while conducting this process far outweighed the risk of moving too quickly. What the CWB quickly realized is that in order to effectively stand up the battalion at this pace, recruiting Soldiers who are up for the challenge of being plank holders is far more important than looking for Soldiers with the perfect "on-paper" credentials. From fresh Cyber Lieutenants assuming the duties and responsibilities of battalion staff primaries to diligent Specialists outfitting the spaces and infrastructure for Expeditionary CEMA Teams, the Army's 915th CWB has evolved from standing up in May 2019 to completing its first overseas multi-national training exercise in September 2019 solely due to the disciplined initiative of a small group of motivated Soldiers.

For the majority of Second Lieutenants, showing up to their first unit means reporting to the Battalion Personnel Office (S1), signing in, and receiving a detailed checklist for how to properly in-process the unit. For 2nd Lt. Amy L'Hommedieu, it meant having to figure out how to do all of that for herself and everyone that would arrive to CWB after her. While much of the unit leadership dove deep into planning for upcoming exercises and events, L'Hommedieu was left to determine what processes and procedures she needed to establish and, slightly more difficult, how to establish them. The unit's new S1 did not wait for someone to tell her what to do; rather, she went out and asked. And asked. And asked. L'Hommedieu spent weeks going from office to office on the installation, acquiring products from other units, and gathering up as much information from as many resources as she could before developing the first 915th CWB Welcome Packet and in-processing checklist. What could have been months of hard learned lessons turned into a few weeks of long days that produced the policies and procedures that allowed the 915th to in-process nearly fifty Soldiers since L'Hommedieu' s arrival. The take-away is this: if you don't know what you don't know, seek out subject matter experts and soak up as much information as you can.

That young officer was enabled to take the initiative that she did by her leadership, who merely gave her a vision and set of priorities. It is a leadership style that Capt. Joseph Lee has eagerly embraced in his S6 shop over the past few months. For the communications team, building a unit from the ground up comes with multiple lines of effort, to include: outfitting a facility with equipment and network connectivity, establishing a training environment, and supporting communication requirements for exercises and operations. In order to succeed in all of these lines of effort, Lee has empowered his, mostly junior, enlisted Soldiers to take the necessary coordination and actions with little oversight. His Soldiers have thrived on such empowerment, managing to outfit a temporary space from which the Battalion can operate, establish a virtual training environment, and support the Battalion's first overseas, multinational training exercise. If asked, Lee contributes his section's success to authorizing his Soldiers to act on his behalf. Instead of needing constant supervision, his junior enlisted now constantly strive to validate their chain of command's trust and respect.

Assuming command of a brand new Company is daunting; doing so while simultaneously preparing that company to participate in multiple training exercises with other well-established organizations is

Continued on page 45

Mission Command in Cyber

By Capt. Jacob Curtis, company commander, Headquarters & Headquarters Company, 780th MI Bde. (Cyber)

Two of the most important principles of Mission Command (ADP 6-0) are disciplined initiative and risk acceptance. These principles are the cornerstones that allow the U.S. Army to be agile, adaptive, and unpredictable on the battlefield. They empower leaders at every level to make difficult decisions in order to exploit opportunities and adapt with the fluidity on the battlefield. Leaders must manage risk and exercise disciplined initiative to capitalize on opportunities to defeat the adversary. While this has been extremely effective throughout the history of conflict, the introduction of a new battle space has caused a regression in this area.

Cyber space is the battleground of the future with engagements happening daily. This new operational environment (OE) is shrouded with mystery and anonymity. It crisscrosses across the global, beyond sovereign borders. This virtual proximity and relative ease of access shrinks the gap between tactical and strategic operations. Add in the cost and sensitivity of the tools to deliver effects and senior leaders start to get nervous regarding the level of potential impact a single Soldier can have in the OE. This results in limited mission command privileges at the lower levels, limiting agility, innovation, and effectiveness.

The ground force commander in battle has the freedom to exercise disciplined initiative and engage the adversary in order to gain ground or other objectives, within the commander's intent. This is in an effort to prevent the time window on such opportunities from closing while reports, requests, and approvals are communicated up and down the chain of command. Commanders must train and trust their subordinate leaders to take every opportunity to win in a complex environment through mission command and not burden them with processes or approvals. The mission and commander's intent should be enough for a leader, at any level, to execute against. The commander must then accept a level of risk that their leaders may take an action that colors outside the lines or does not pay off, but training, certifying teams, and involvement enables commanders to have a good understanding of that level of risk.

Cyber teams are well trained, certified regularly, and commanders are deeply involved, yet there are simple tasks, like scanning a target, that is overburdened by processes and approvals before execution. An action that any person, with no training, can execute from the comfort of their home against the same target without breaking any laws. This stifles the flow of battle as we maneuver through the networks of an adversary, coming across a target of opportunity that was not preapproved. Sure, there are different types of missions that may require more sensitivity but we are the U.S. Army, not a three-letter agency, we operate in the open. Our adversaries may not see us coming but they know when we get there.

A majority of Cyber missions deliver non-lethal effects. In a ground battle, the decision to deliver a lethal effect is trusted to a Soldier of any rank. Why? Because they are trained to use their weapon system, react appropriately in a chaotic environment, and operate within rules of engagement. So why can't a Cyber Soldier deliver a non-lethal effect against a target without a significant bureaucratic process? They are trained on their weapon system and they operate in a more complex environment. It seems to be a fear of the unknowns, the fear of losing capability, or the fear of losing a firing platform. The Army thrives on the unknowns because of mission command. We are given intent and thrown into battle. The freedom to react to the unknowns, fighting towards meeting the intent enables the agility needed to win. Capability for the Army has always been its people, it's hard to lose capability in Cyber. Tools may become ineffective but given the freedom to innovate, Soldiers will find a way. For Cyber, a firing platform is any device connected to the internet and with over 22 billion devices on the internet and the advent of

Continued on page 46

174th Cyber Protection Team fights online battle

Sgt. Nathaniel Free, Utah National Guard

DRAPER, Utah -- Eighteen Soldiers assigned to the Utah Army National Guard's 174th Cyber Protection Team prepare to deploy from Draper, Utah, Jan. 2, 2019. The 174th's mission is to mitigate the enemy's ability to affect operations in the cyber domain. (Photo Credit: Sgt. Nathaniel Free)

DRAPER, Utah - It was a hot Saturday afternoon in July 2005. U.S. forces quickly surrounded an internet café on the outskirts of Baghdad and captured an al-Qaida courier outside. An email was recovered, signed by the terrorist network's then second-in-command, Ayman al-Zawahri, who was hiding deep in Pakistan. The email was addressed to the al-Qaida leader in Iraq, Abu Musab al-Zarqawi, known as the "Sheikh of the Slaughterers."

In the email, Al-Zawahri outlined a step-by-step plan to expel Americans from Iraq and establish a caliphate. Part of that plan was focused on a new battlefield.

"I say to you," Al-Zawahri wrote in Arabic, "that we are in a battle, and that more than half of this battle is taking place online."

It was a call to action.

More than a decade later, 18 Utah Army National Guard soldiers from the 174th Cyber Protection Team departed from Utah National Guard Headquarters in Draper, headed to Fort Meade, Maryland, to join the online battle as part of Task Force Echo III.

The task force consists of 12 states working together under the 126th Cyber Battalion based out of Massachusetts. The team will be defending the continuity and stability of U.S. infrastructure during its 400-day deployment.

"We live in an increasingly complex world," Maj. Gen. Jefferson Burton, adjutant general of the Utah National Guard, said during the team's departure ceremony. "This nation is much more difficult to defend than it was a couple of years ago."

He said that while Fort Meade might not be the deserts of the Middle East, the cyber domain is equally important, if not more so.

"There are vulnerabilities in any system," said Cpt. Brandon Morris, commander of the 174th Cyber Protection Team. "We're mitigating the enemy's ability to affect operations in the cyber domain -- both military systems and civilian systems."

To put it simply, the 174th Cyber Protection Team will be defending the American people on the homefront. Wake up and flip a switch, a light will come on. Turn a lever, water will flow from a faucet. Drive to work, lights change from green to red.

"This particular unit is composed of skilled professionals in the cyber realm," Burton explained. "And they do battle with keystrokes."

According to Morris, the 18 soldiers trained three years to prepare for this deployment.

"As far as the overall technical competence of our team, I can safely say that we are the strongest of all the states," said Cpt. Kylie Boyle, the senior officer in charge of the 174th Cyber Protection Team. "We specifically focus on defensive cyber operations. There's a lot of critical infrastructure-hardening."

Continued on page 44

Cyber program graduate discusses fast-track to becoming an officer

U.S. Army News Service

FORT GORDON, Ga. – *The Cyber Direct Commissioning Program allows talented civilians a fast track to becoming an officer, attracting qualified civilian professionals to help the Army develop and execute programs and equipment to support its operations in cyberspace. Pictured here, 1st Lt. Ryan Greer graduates Basic Officer Leader Course (BOLC). (courtesy photo)*

WASHINGTON -- Since late 2017, the Cyber Direct Commissioning Program has allowed talented civilians a fast track to becoming an officer, attracting qualified civilian programmers, software engineers, developers, and data scientists to help the Army develop and execute programs and equipment to support its operations in cyberspace.

This program has given qualified individuals the opportunity to join the Army as first lieutenant. On top of that, they may be eligible for a student loan repayment of up to $65,000 over the course of the officer's initial three-year term. Most applicants can be categorized as prior-service enlisted military personnel, government employees and contractors, private sector workers, and academics.

1st Lt. Ryan Greer is one such individual who successfully completed the Cyber Direct Commissioning Program, taking his professional goals and ambitions to the next level.

At what point in your life did you realize you wanted to join the Army and be part of something big?

"As far back as I can remember, I have wanted to be part of something bigger than myself. However, it was only a few short years ago that I started to see the Army as the organization for me."

Everyone's path to becoming commissioned is unique; what was the process like for you?

"For me, the process started a couple of years ago. I had recently become a volunteer firefighter and was looking for other ways to serve while still progressing my career as a software developer. I was considering applying for OCS when I came across the Cyber Direct Commissioning program on GoArmy.com."

"After thorough consideration, I decided this was a great opportunity for me to use my civilian skills to serve my country. I applied for the program in July 2018, interviewed over the phone shortly thereafter, and interviewed on site in Fort Gordon that August. I was selected in September 2018 and went to MEPS not long after. Between October and December I completed the paperwork and left for Fort Benning (DCC) in January 2019."

What was the most challenging aspect of BOLC and how did you overcome it?

"Overall my experience at BOLC was positive and I relied heavily on my peers to help me overcome challenges. With that in mind, adapting to the increased responsibility of being an officer with the loss control inherent to being in the Army has been the most challenging aspect."

What can you tell us about your upbringing and how it shaped your Army career?

"I grew up with both parents working in public service. They showed me that it is more important to serve others than myself. If not for the example set by my mother and father I would not have considered the Cyber Direct Commissioning program."

What character trait or professional skill that has helped you the most?

"I believe integrity to be the most important character trait one can have. I also believe that the ability to see the bigger picture while understanding the details will be a great asset in my career. I have the ability also have an ability to quickly understand existing

Continued on page 46

New 780th MI Brigade NCOs take the oath to become

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

FORT GEORGE G. MEADE, Md. – *The 780th Military Intelligence Brigade (Cyber) hosted a Noncommissioned Officer (NCO) Induction ceremony for 27 NCOs at the Post Theater on October 16 in order to "charge" them with their increased duties and responsibilities as detailed in the Creed of the Army NCO and the NCO Charge. (U.S. Army Photo)*

FORT GEORGE G. MEADE, Md. – The 780th Military Intelligence (MI) Brigade (Cyber) hosted a Noncommissioned Officer (NCO) Induction ceremony for 27 NCOs at the Post Theater on October 16 in order to remind them of their increased duties and responsibilities as detailed in the Creed of the Army Noncommissioned Officer.

Command Sgt. Major James Krog, the senior enlisted leader for the 780th MI Brigade, was the guest speaker, and he was accompanied by the other senior NCOs in the official party including Command Sgt. Maj. Kelly Barnes, the senior enlisted leader for the 781st MI Battalion (Cyber); Command Sgt. Maj. Sean McNamara, senior enlisted leader for Task Force Echo III; and 1st Sgt. Stanley Collins, Headquarters & Headquarters Company, 780th MI Brigade.

In addition to reciting the NCO Creed, the inductees learned about the history of the NCO Corps. Staff Sgt. Jacob Starling, the narrator for the ceremony, said the American Noncommissioned Officer tradition began with creation of the Continental Army in 1775. Starling told the audience that Gen. George Washington, the commander of the Continental Army, believed the Army's leadership, including commissioned and noncommissioned officers, was a major weakness, and after Valley Forge, Gen. Washington turned to a Prussian military officer, Baron Friedrich Wilhelm von Steuben, to instill discipline and military training into his Army.

Starling said Baron von Steuben's influence extended beyond the war. Baron von Steuben's drill manual, "Regulations for the Order and Discipline of the Troops of the United States", published in 1779, was the basic training guide for Washington's Army. The "little blue book" standardized NCO duties and responsibilities and became the primary regulation for 33 years and it emphasized the "need to select quality Soldiers for NCO positions".

Starling also told the inductees that the word "sergeant" is a French word which means a "servant, a valet or a court official." All of these words derive from the Latin term "serviens,"

Cpl. Matthew Taylor, from Simi Valley, California, described what it meant to him to be an NCO.

"Being an NCO means taking responsibility and looking after those who you are in charge of. Primarily, it is putting others before yourself," said

‘servant leaders’

Taylor. “It’s a very humbling experience and a major responsibility.”

Taylor wanted to recognize Sgt. Kyler Kline, Staff Sgt. Christiane Roberto, and Staff Sgt. Starling, as the NCOs who have inspired him because those three NCOs were “great influences on the kind of leadership I’ve seen that I want to exemplify.”

Specifically, the traits those three NCOs personify was “Being fearless in the face of adversity. Fighting for those who you lead even if that means going up against the people in charge of you,” said Taylor. “Fighting for what’s right, for what your Soldiers need and putting their needs above your own.”

Congratulations to Cpl. Taylor and the other 26 new NCOs: Sgt. Matthew Alderman, Sgt. Brandon Bissett, Sgt. Tanner Carr, Sgt. Janice Davis, Sgt. Joshua Day, Sgt. Thomas Fazio, Sgt. Tyler Hornbeck, Sgt. Samuel Idoni, Sgt. Duncan Jentzsch, Sgt. Justyn Johnson, Sgt. Kristopher Joyce, Sgt. Alan Kim, Sgt. Keefe Matson, Sgt. Stephen Paradis, Sgt. Cristian Perez, Sgt. Alex Prufer, Sgt. Jaslyn Riat, Sgt. Ryan Riebling, Sgt. Jiseng So, Cpl. Matthew Taylor, Sgt. Rodrigo Valdes, Sgt. Grant Ward, Sgt. Scott Wareham, Sgt. Marlin Washington, Sgt. Kristian Winslow, Sgt. Adam Wong, and Sgt. Jonathan Woods.

The Soldiers and Army Civilians of the 780th Military Intelligence Brigade (Cyber) wish them all the best.

FORT GEORGE G. MEADE, Md. *– Command Sgt. Maj. Kelly Barnes (right), the 781st Military Intelligence Battalion (Cyber) senior enlisted leader and its “Keeper of the Colors”, returns the colors to 1st Sgt. Stanley Collins, who was the acting command sergeant major, at a Change of Responsibility ceremony in the post theater, October 10. (U.S. Army Photo)*

FORT GEORGE G. MEADE, Md. *– Sgt. Tyler Hornbeck stands in the arch of the Noncommissioned Officer (NCO) during an NCO Induction ceremony hosted by the 780th Military Intelligence Brigade (Cyber) at the Post Theater on October 16. (U.S. Army Photo)*

Disciplined initiative and risk acceptance

By Sgt. 1st Class Shtina Love, 780th MI Brigade Sexual Harassment and Assault Response Coordinator

Praetorians! I am Sgt. 1st Class Shtina Love, your Brigade Sexual Harassment and Assault Response Coordinator (BDE SARC). I have been with the unit since May 2018 and have exercised disciplined initiative on several fronts. I use my passion to help others through volunteering in my message of lifestyle change to foster culture change.

My first assigned position had limited expectations and was over strength; however, I observed a section understrength with tremendous output. I offered my services in management and communications, which improved our overall efficiency. I was fortunate; they were so receptive. Later another opportunity arose as the gap I once filled received an increase in members.

I am a trained DoD Sexual Assault Prevention and Response (SAPR) Victim Advocate (VA) since 2014. I have served in brigade level and below positions ensuring to remain active in the program at each duty station. It takes discipline to maintain your credentials, CEUs, and knowledge with this program. They are constantly working to ensure we provide the best services and products to our clients. I disclose my capabilities upon arrival informing my new command that I am an asset for use within the organization. I served as a collateral duty VA since arrival, but had no clue I would soon join the BDE SARC and VA as a valued member of the team. Each VA has a unique way of conveying the policies governing sexual assault and harassment such as different leadership styles. I am a community based VA with a focus on travel, smiles, food, and happiness. Genuinely caring about one another will help us with bystander intervention. The act of recognizing something is wrong, take responsibility for it, and acting accordingly to deescalate a situation requires a varying levels of risk. The same holds true for joining the military but the benefits far outweigh most of the risks.

The veterans of our past, present, and future also displayed their disciplined initiative by heeding our nation's call and bore some tremendous risks as they fought through a myriad of war and/or conflict. Some veterans did not make it home, some are home but wish they were not, many are home with support, but there are many without.

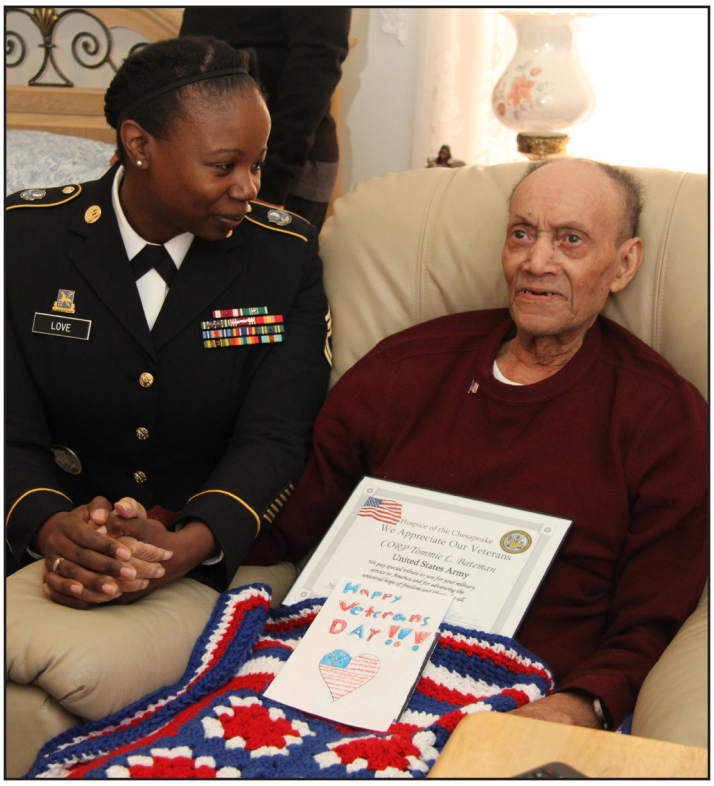
Herein lies another opportunity to intervene with little calculated risk and an opportunity to make a positive impact on another's life. I enjoy spending time with veterans and sharing stories from their past. It is a free lesson on truly living. I try to take every opportunity to engage with these remarkable humans. I seek community activities that celebrate the contributions of our veterans such as the women of the 6888th Central Postal Directory Battalion.

The 6888th was the first and only all-Black female Women Army Corps (WAC) unit deployed overseas during WWII. The unit was active from 1945 to 1946 and consisted of 855 women under the Command of Maj. Charity Adams. Their nickname was "Six-Triple Eight" and their motto was "No Mail, Low Morale."

Continued on next page

Sgt. 1st Class Shtina Love (left) with Pfc. Delores Ruddock, a WWII Veteran, whom served in the 6888th Central Postal Directory Battalion in Europe, shown here during a community celebration of women veterans. (Courtesy photos)

Continued from previous page



Sgt. 1st Class Shtina Love (left) visits with Cpl. Tommie Bateman, a Korean War veteran, whom she visited as part of the Honor Salute program with the Hospice of the Chesapeake.

I also volunteer with the Hospice of the Chesapeake, https://www.hospicechesapeake.org, in support of one of their programs. They collaborate with local Military Volunteers to provide Honor Salutes for veteran patients. The Honor Salute is the backbone of their Veterans Program. It is our way of saying Thank You to veterans for their service, while they are still with us. We want them to know how much we appreciate their sacrifices and will never forget.

A group photo from another Honor Salute event to showcase that all branches of service volunteer with the Hospice of the Chesapeake.

How do you exercise disciplined initiative and risk acceptance?

Hastati 7 says...

By 1st Sgt. Stanley Collins, HHC, 780th MI Bde. (Cyber)

We have all heard the stories about Sergeants Major telling people to stay off their grass. I have never actually seen it before, but I know where they are coming from. Why would someone be so particular, serious, and strict about something seemingly so trivial? Why does the grass matter? Does the Sergeant Major just want to be persnickety about something? Does he just want to yell? Who is he trying to impress?

It is not about the grass. It is about not taking short cuts and adhering to standards. Everyone doing things the right way is part of what sets great organizations apart from good ones. Organizations have to have clear, known standards to operate effectively. The discipline to adhere to, the selflessness to take the time, and the commitment to ensure completion and accuracy of a process is crucial for excellence. Processes and standards are part of what holds a team together. It is setting and meeting expectations. A Sergeant Major ensures known standards are met and sets other standards for their unit. They make a unit more efficient and most of all, capable.

I want our grass green, thick, and looking good…and I want to keep it that way. The grass is the standards I have been charged to make and uphold. It is choosing the hard right over the easy wrong. Our grass is every process which keeps things efficient. It is taking care of Soldiers and Civilians on my team regardless of anything. I WILL NOT cut corners. I WILL NOT let the little things slide. I WILL meet the standard and hold others to the standard every day. The mission, the unit, and our teammates are worth it. I am too. Now, let us keep that grass looking good and tell others the same thing. No shortcuts!

Faith and Risk Taking

By Chaplain (Maj.) Peter Baek, brigade chaplain, 780th Military Intelligence Brigade (Cyber)

***FORT GEORGE G. MEADE, Md.** – Here is your 780th Military (MI) Brigade (Cyber) Unit Ministry Team at Fort Meade (from left to right) Chaplain (Maj.) Peter Baek, Brigade Chaplain; Staff Sgt. Patrick Grill, brigade chaplain assistant; Chaplain (Capt.) Michael Cerula, Battalion Chaplain, 781st MI Battalion (Cyber), and Pvt. Nakoya Davis, battalion chaplain assistant. (U.S. Army photo)*

King Solomon, considered the wisest person ever lived, wrote, "A prudent person foresees danger and takes precautions. The simpleton goes blindly on and suffers the consequences" (Proverbs 22:3).

Life is full of risks, and missing the opportunity to take some of them could lead to much regret in the end. Taking risks takes faith. You can say faith cannot exist without a little bit of risk.

We all have taken some sort of risk in our lives and in careers. At some point we have decided to leave our comfort zone to take on new challenges: a new opportunity, adventure, position, or even a new relationship perhaps…

Risk taking can be daunting, even paralyzing, but as long as we are assured that it is God's perfect will for us and we know God has our backs He will turn risks into rewards.

King Solomon writes in Proverbs 3:5-6, "Trust in the Lord with all your heart, and do not lean on your own understanding, in all your ways acknowledge Him and He will direct your paths." What could be a more fitting picture of risk taking?

However, it is also important to remember that as we face risks, God also urges us to practice a leveled amount of wisdom to balance things out. Blind faith is not just risky. It's also uncalled for. King Solomon again writes in Proverbs 11:14, "For lack of guidance a nation falls, but victory is won through many advisers."

***WASHINGTON, D.C.** – Soldiers and their Families, representing the 780th Military Intelligence Brigade (Cyber), attended a reception and dinner for service members and their Families in honor of Military Family Month at the Vice President's home at One Observatory Circle NW, on November 6 (Courtesy photo)*

Disciplined Initiative, Risk, and Legal Compliance

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

ADP 6-0 is the Army's doctrine of Mission Command. It explains that "Commanders accept prudent risk when making decisions because uncertainty exists in all military operations. Prudent risk is a deliberate exposure to potential injury or loss when the commander judges the outcome terms of mission accomplishment as worth the cost… Reasonably estimating and intentionally accepting risk are not gambling. Gambling, in contrast to prudent risk taking, is staking success on a single event without considering the hazard to the force should the event not unfold as envisioned."

Ultimately, it is the Commander – not his staff or subordinates – who are responsible for assessing the risk and determining the prudence of a course of action. The Commander must not be overly conservative and seek to eliminate all risk; but he must also not be reckless. Command is neither a license to be timid, but it is also not a license to Leroy Jenkins recklessness. The United States expects her officers to demonstrate audacity, constrained within the bounds of law, ethics, and good sense.

FORT GEORGE G. MEADE, Md. *– Lt. Col. Gaetano Snow, the brigade S3 (operations) officer, 780th Military Intelligence Brigade (Cyber), was promoted to lieutenant colonel at an event hosted by Col. Brian Vile, the brigade commander, at Club Meade, October 4. (U.S. Army Photo)*

In our previous entry into The Byte, my colleague Frank Colon discussed how the process of ensuring legal compliance is designed to ensure that the Commander maintains freedom of action by ensuring "innovation complies with standards and controls." Failing to do so might mean good, creative ideas are suffocated before they can take root. Most of these rules exist for reason. Our intelligence oversight regime, for example, came from the abuses of military (and civilian) intelligence agencies in the 1970s, where the power of the military was directed towards American citizens. These were later determined to be abuses of the First and Fourth Amendments to the Constitution, since they targeted Americans on the basis of their political beliefs, and sometimes without any cause at all. These abuses by the military and our interagency brethren resulted in the intelligence oversight regime by Congress and the Executive Branch. One could easily envision scenarios where our current authorities were taken away from us if we did not show ourselves worthy of the trust and confidence the Nation placed in us.

Legal standards exist for a reason; rightly the former Secretary of Defense exhorted us to "play the ethical midfield." A commander owns the operational risk – he alone is responsible the mission's failure or success. But no commander will rightly disregard legal risk – if an action is not moral, ethical, or legal it is not his risk to assume.

Recently I heard a senior NCO describe a good NCO as one who "once you explain why, he does what you tell him." I must respectfully but forcefully disagree with this NCO. A good Soldier – whether officer or enlisted – is one who complies whether or not he understands or agrees with his Commander. It is a Commander's responsibility to communicate his desired end state to his subordinates so that they too may exercise their initiative to accomplish his goals. But once that end state is communicated – in the absence of an illegal, immoral, or unethical order – it is the subordinate's responsibility to comply regardless of our personal feels about that order. Good order and discipline demands nothing less.

Why I Stay...In the Fight!

Sgt. Devin Aikens, Headquarters & Headquarters Company, 781st Military Intelligence Battalion (Cyber) Vanguard!

MOS: 17C – Cyber Operations Specialist

Position: Battalion Executive Assistant and BOSS Representative

Hometown: Boynton Beach, Florida

"In 2013, I joined for education, guaranteed income, and to travel. Some would say I joined for myself. Over the years, I have done all those things and then some. If people were to ask me what made me stay in the Army, I'd say Jesus Christ, the experience, the fellow Service Members, and the opportunity to serve the nation."

Did anyone (or group of people) influence your decision and why?

"Jesus Christ influenced my decision to stay in."

What are your career goals and future aspirations?

"My future aspirations are to become an awesome officer in the U.S. Army, creating effective and positive change for all Soldiers in my sphere of influence, and to be a great role model for all Service Members, even those who are considering joining the service."

FORT GEORGE G. MEADE, Md. *-- Sgt. Devin Aikens, a cyber operations specialist (17C), assigned to the 781st Military Intelligence Battalion (Cyber) reenlisted in a ceremony hosted by the battalion commander, Lt. Col. Nadine Nally, at the Post Theater October 15. (U.S. Army photos)*

780TH MILITARY INTELLIGENCE BRIGADE RETENTION TEAM

Senior Career Counselor
Sgt. 1st Class Antoinette M. Pickett
Commercial: 301-833-6405

781st Military Intelligence Battalion
Career Counselor
Staff Sgt. Adam Meston
Commercial: 301-833-6410

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

Photos

FORT GORDON, Ga. *-- Maj. Rose Abido (right), the battalion S-3 (operations), 782nd Military Intelligence Battalion (Cyber), and Command Sgt. Maj. (retired) Thomas Clark, the former senior enlisted leader of the Signal Center of Excellence, and currently serving as the liaison between the Augusta Community and the Cyber Center of Excellence – Fort Gordon are shown here at the Christmas House Opening Ceremony on November 14. (Courtesy photo)*

Hackathon

ODENTON, Md. *-- The 780th Military Intelligence Brigade (Cyber) partnered with Anne Arundel County Public Library to host a 'Hackathon' event for teens at the Odenton Regional Library on November 12. Read the story on page 41.*

Winterizing your car

By Brian Sylvester, 780th Military Intelligence Brigade Safety and Health Occupational Specialist

Ready for winter? Get your car ready, too. Here's what you need to know for tire maintenance and a look under the hood. Have your kids prepare a winter safety kit, and remind your teen of winter driving tips.

Tire Maintenance

Rain, snow and ice reduce tire traction and compromise your control. What's the solution?

1. Get winter tires

Winter tires dig into loose snow and compress it into their large tread grooves (like packing a snowball), resulting in snow-to-snow traction.

You can choose from three types:

- High performance winter tires were originally designed to meet strict government regulations for driving on high-speed highways in Europe. They feature large directional and/or asymmetric treads to enhance handling and steering, resist hydroplaning and help tires work through slush.
- Studless winter tires are most common and increase traction on ice through the use of advanced tread rubber compounds. They're a safe alternative to studded tires, which are forbidden in many states.
- Studdable winter tires are popular for light truck owners and drivers who spend a lot of time on snow and ice-covered roads. Small carbide pins ("studs") that chip into ice can be inserted by your tire specialist.

2. Check your tire pressure

Fall and early winter are the most critical times to check tire inflation pressures because the days are getting shorter and temperatures are getting colder.

Tip: For every 10-degree Fahrenheit change in temperature, your tire's inflation will change about one pound per square inch (psi) (up with higher temperatures and down with lower).

Tip: Check your tire pressure in the morning before you drive a few miles. If you park in an attached or heated garage, you will "lose" pressure when you leave its warmth.

3. Check your tire treads and sidewalls

Look for thin or uneven tread wear. Take a Lincoln-head penny and insert it Lincoln-head first into your tire tread at the most worn part of the tire. If you see the top of Lincoln's head, you may need new tires. Cut or damaged sidewalls are also weak areas that can collapse under severe conditions.

Under the Hood

1. Check your battery

It takes a lot more power to start your car when it is cold outside. Check for clean and tight connections and proper fluid levels. Clean corrosion (a whitish powder) from battery terminals.

2. Check your cooling system

Your coolant system keeps your car warm. Check the level, acidity and concentration of radiator fluids at least every 3,000 miles.

Tip: A mixture of 50% anti-freeze and 50% water will protect down to -40 degrees Fahrenheit.

3. Clean your fuel system

Add a de-icer to your fuel to keep moisture in the fuel system from freezing.

4. Change your oil and oil filter

Check your owner's manual for the grade of oil recommended for winter. In most cases, 10w30 oil works year-round.

5. Inspect and replace

Inspect your air filter, rubber hoses and drive belts and replace as necessary. Also check your fluid levels (transmission, brake, differential, power steering and window washer fluid).

The Nibble (continued)

Continued from page 6

While these proposals raise several questions not addressed in this article, modifying current training and employment models provide viable professionalization paths that facilitate coordination across OCO and DCO missions. Additionally, these actions would build technical skill and experience within the force which is required to exercise disciplined initiative. This added level of proficiency within specializations further empowers commanders to widen their risk acceptance aperture, enabling dynamic mission growth and execution against a range of adversary targets and threats.

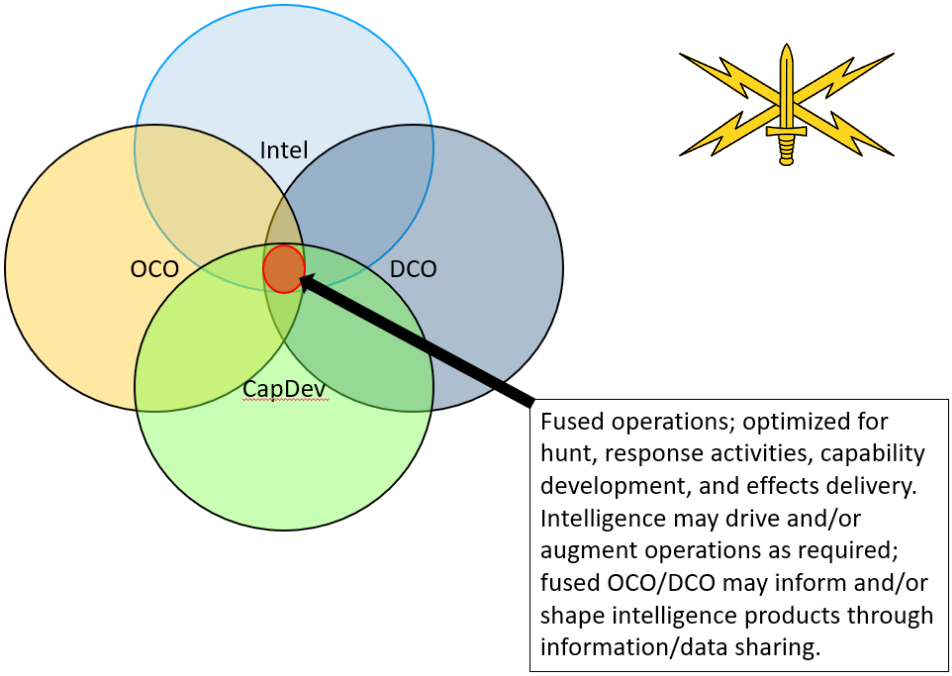
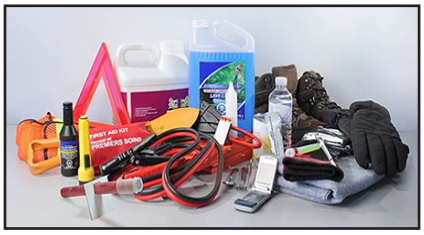


Figure 2: Operational employment should be fused across OCO, DCO, Intelligence, and CapDev.

Winter Safety (continued)



Winter Safety Kit

Prepare a winter safety kit to keep in your car at all times. Be sure to include:

1. Winter necessities such as an ice scraper; tire chains; extra washer fluid; boots and gloves; and sand, kitty litter or old house shingles for traction.

2. Emergency supplies such as extra clothing and blankets, flashlight with spare batteries, energy bars or dried snacks, drinking water, a battery-powered radio with spare batteries, a first aid kit, booster cables, safety flares, a small shovel, and a jug of water and funnel for radiator refills.

3. Tools and "fix-it" supplies such as a screwdriver, pliers, rubber hammer, wrench, a can of penetrating oil, an old scarf and belt for emergency hose repairs, and a small throw rug and old shower curtain (for kneeling next to your car or getting under it).

Winter Driving Tips

No matter how safe your car is, winter driving requires extra attention. Brake gently, accelerate gently and steer gently. Remember these tips, too:

Tip: As every driver's education teacher repeats, steer into a skid.

Tip: If you get stuck in the snow, throw kitty litter, old newspapers or dirt in front of and behind the drive wheels.

Tip: In snowy conditions, drive in lower gears. Avoid using your overdrive feature.

Tip: Always keep your gas tank at least half full.

780th MI hosts free, educational hackathon

By Maya Jordan, Fort Meade Soundoff!

***ODENTON, Md.** — Soldiers and Army Civilians from the 780th Military Intelligence Brigade (Cyber) partnered with Anne Arundel Community Public Library to host a 'Hackathon' event at the Odenton Regional Library on October 8. The Maryland STEM Festival event was organized to encourage teens' interest in STEM activities. (U.S. Army Photos)*

ODENTON, Md. – What do you call a conference room filled with curious students, military cyber professionals and computers? A hackathon.

Soldiers of the 780th Military Intelligence Brigade (Cyber) hosted the free, educational hackathon on Sept. 10 at the Odenton Regional Library.

The hackathon is the first of three monthly programs in partnership with the Maryland STEM Festival at the library that celebrates teaching science, technology, engineering and mathematics. The library has been in partnership with the Maryland STEM Festival since 2015.

"STEM programs are part of our extensive educational offerings that serve babies to seniors," said Christine Feldman, communications specialist for the Anne Arundel County Public Library. "Our mission at the library system is to educate, enrich and inspire the residents of Anne Arundel County.

"STEM knowledge is vitally important for the future of our country. We regularly offer STEM programs for preschoolers, school-aged kids, teens and adults throughout the year, but give special focus during Maryland STEM Festival month."

The hackathon featured seven demonstrations with about 11 mentors providing instruction and guidance.

The hands-on learning session was organized by 2nd Lt. Alan Baily, 780th MI planning specialist, who provided instruction and supervised the station activities.

"A hackathon is a pretty ambiguous term," Baily said. "It's really hard to define. We decided to focus on some of the basic cyber security principles that a lot of hackers use -- whether that is password cracking, web server proxies or a myriad of different tools the students can use."

Baily outlined the process.

"First, start out with demonstrations and explain the ethics behind each," he said. "The intent is to show the students what is actually available and the [outcomes]."

Ultimately, a hackathon event is an opportunity to facilitate science, technology, engineering and mathematics teaching and experiences through

***ODENTON, Md.** — Chief Warrant Officer 4 James Richards, 780th Military Intelligence Brigade (Cyber), was the mentor for the Password Cracking station at a 'Hackathon' event at the Odenton Regional Library on October 8.*

guided computer simulation followed by replication.

The event also exposed students to procedures for safeguarding computer usage while introducing them to various fields of information technology.

The 780th MI provides support to the Anne Arundel County Library as a way to enrich, expose and educate the community to STEM with recurring, free educational events.

Many parents were elated to have their children participate in the event.

"I found out about this event from the library for my son, Gabriel," said Jacqueline Till Graham, a retired master sergeant from the 902nd Military Intelligence S5 Logistics unit. "He attends Arundel Christian School. They do not have a [full] STEM curriculum, but they just started a computer programming class."

During the three-hour event that started at 4 p.m., students rotated from station to station.

One station, "Cracking the Perimeter," received lots of attention from the participants. Students learned how security is evolving in the cyber industry and moving away from past technologies.

The demonstrator explained how wireless networks in a home network for students can be unsafe and why modern wireless practices are moving to WPA2 as a more secure tool.

At the "Password Cracking" station, students learned the basics to hacking a password.

Chief Warrant Officer 4 James Richards of the 780th MI, who pursued an undergraduate degree in computer science prior to joining the Army's Signal Corps, outlined the importance of safeguarding passwords for websites, smartphones and internet connectivity.

"If you are trying to make a secure password, make it long," Richards said. "It does not need to be complicated. There's a website called 'How secure is my password?'

"You can use it at home to check how secure your password is."

At the binary station, 2nd Lt. Rebecca Acheson of the 707th Communications Squadron displayed a simulation that resembles a video arcade game.

The game allows participants to learn how computers communicate through binary code, which included

ODENTON, Md. — *Robert Inghat, an Army Civilian assigned to the 780th MI Bde. (Cyber), was the mentor for the Capture the Flag station at a 'Hackathon' event at the Odenton Regional Library on October 8.*

numbers and letters.

"[With] this binary game, you have different numbers: binary, hex and octal," Acheson said. "[Then] you have to try and make the number you see on the screen.

"If it is a binary number -- 1, 2, 4 or 8 -- you have to go to the right. And if you hold left, you use numbers 16, 32, 64 and 128."

Career opportunities within STEM fields are growing in demand. According to data from the Pew Research Center, since 1990 employment in STEM occupations has grown 79 percent, increasing from a workforce of 9.7 million to 17.3 million.

"Having the opportunity to influence students, whether they pursue a career in the Army, is not the goal," Baily said. "[The goal is] to get them excited about what we do."

Early exposure to STEM activities can lead students into pursuing STEM careers.

The Steganography station allowed students to decode messages that had been embedded through other files such as PDFs or photos.

Lyam Harbaugh, 15, a home-schooled student who runs a computer technology business, was enthusiastic about the hands-on activities.

"It's been a year now [that I've been] coding stuff," Lyam said. "My dad works in this field, so he's been teaching me about [computers] all my life."

AvengerCon IV (cont.)

Continued from page 24

"challenges" and events hosted by the facility looking at specific cybersecurity issues. These include critical infrastructure security events simulated in "Dream Valley," a scale model village connected to actual industrial control systems and other operational technology.

DreamPort's planned expansion is probably a good thing, considering how AvengerCon has grown. In the past, the event was limited to Army personnel, but now it includes attendees from across the Department of Defense and other government agencies tied to cyber operations, as well as students and representatives of industry.

"We felt we needed to branch out and start making sure that we are supporting the community better each year as we expand," said Seiler. "The growth is great, but it also brings in other woes and requirements." The logistics of getting people onto Fort Meade was one of them, Seiler explained—while it provided a natural level of security around the event, using the base made drawing on outside resources difficult and limited who could be brought in to attend.

"We found it works better if it's off base," he said.

Using DreamPort opened up the opportunity to add resources provided by outside organizations that "connect to our mission," Seiler said. Those included the "villages" at the event brought in by security community organizations—including ICS Village's industrial control systems "capture the flag" competition (in which attendees looked for ways to compromise simulated plant hardware) and the Voting Village's collection of voting-machine hardware and exploration of election security.

"The election thing was nice to have," said Seiler. "I don't know if it was our big thing, but lots of people are talking about it... it sparks conversation, which was the intent of accepting something like that. That's the intent of all the villages—to build the conversations."

The additional space allowed for the expansion of AvengerCon's training workshops, which included day-long classes in reverse-engineering and software "fuzzing." Additionally, the event hosted a simulation called "The Day After"—in which teams from the US Naval Academy, James Madison University, American University, and the University of Maryland, Baltimore County, simulated strategies for government agencies to respond to a large-scale cyberattack on the United States.

The success of AvengerCon has prompted plans to replicate it in some form for the military and intelligence cyber community at Fort Gordon in Georgia. But the organizers also want to make sure that AvengerCon itself doesn't outgrow its grassroots, community feel. They also want it to stay focused on its mission. That fits into the overall USCYBERCOM strategy for DreamPort, which has an ongoing calendar of highly focused events surrounding the command's "Persistent Innovation" strategy.

"You know that cyberspace is under constant change," said Luber. "It requires us to constantly innovate, and innovation just doesn't happen in government. It's also happening in industry, academia. We need a place to work, we need a place to meet, and we need a place to innovate, and DreamPort provides that combination for us."

In addition to providing an environment for academic outreach to high schools and universities, Luber said DreamPort is "a mission accelerator, an incubator for US Cyber Command where projects are conducted with the goal of completing those projects within 90 days. So think of that innovation process where you've got an idea, you've got a concept, you want to run it quickly, and if you fail, you fail fast. And if you succeed, you've moved to the next step where you try and get it to operational capabilities."

Conducting those projects in an unclassified environment, Luber said, encourages the sharing of ideas and speeds up the creation of new solutions to cyber security issues.

Some of those projects include rapid-prototyping events in which "we bring industry partners in from all different sizes, small businesses, large businesses, and then have them work the problem,"

Luber explained. "We've had six rapid-prototyping events over the course of the past year. We've seen even one-person companies outperform some of the

Continued on the next page

Continued from the previous page

bigger prime contractors that you might think that we're dealing with on a regular basis."

One of DreamPort's recent rapid-prototyping events was run by USCYBERCOM in partnership with the Office of the Secretary of Defense for Small Business and Manufacturing. It focused on protecting the security of small businesses within the Defense Industrial Base (DIB) with the application of "zero trust" network security, which is an architectural approach to handling application and information security that would help protect their security regardless of the overall security of the network environment.

The project looked at ways to apply zero-trust architecture, not just to the DIB, but to Department of Defense information systems and networks as well. "By bringing together talent from DISA, NSA, USCYBERCOM, and industry, we were able to really work on some interesting prototyping activities, and it's going to help us drive the future for the Department," Luber said.

B/781 MI BN -- Changing the Culture of Cyber Training (cont.)

Continued from page 13

increases the ability for Leaders to project readiness, and optimizes cost. It additionally provides defined timelines for ADCON (administrative control) required training to the OPCON (operational control) chain of command for mission deconfliction. Army adjunct offerings prevent unpredictable circumstances from disabling the system. It additionally affords ADCON leadership insight into the number of adjunct requirements within their formations to maintain adequate throughput.

As with any proposed change to a familiar system, the cohort method is not infallible. Leaders would accept the following significant risk factors: minimal numbers of empty seats are unavoidable; OPCON leaders will loose significant numbers of personnel cyclically; and personnel may wait months to attend training based on arrival date and schedule of courses.

Continued on the next page

Continued from the previous page

The consistently and predictability of the cohort delivery model can outweigh these factors when evaluated holistically. Additionally, with the recent JQR based training certification, smaller numbers of personnel would require the entirely of the J7 pipeline, further decreasing risk.

The future of USCYBERCOM and T10 cyberspace operations is determinant on a substantial decision: to split, or not to split from the NSA. Prior to the approval of such verdict, we can exercise disciplined initiative and accept risk within the realm of cyber training. A cohort training methodology dissolves ourselves of by-name requirement tracking at the Army Cyber Command level, enables lower level leadership to develop internal adjunct instructors for emergent requirements, and foundationally increases predictability in a multitude of factors.

C/781 MI BN -- Discipline, an essential element (cont.)

Continued from page 14

Increasing the periodicity and toughness of situational training exercises for cyber Soldiers will improve their mission effectiveness, build confidence, and instill discipline. Cyber has not eliminated the Army's need for tough realistic training, but instead increased its importance in building mentally tough and resilient Soldiers. Winning in cyberspace will require continuous realistic training that continuous live operations cannot provide.

174 CPT fights online battle (cont.)

Continued from page 29

The benchmark qualification for cybersecurity operators is the Certified Information Systems Security Professionalism certification, Boyle said. It's one of the most challenging certifications in information technology. The exam alone is six hours long, so it's no small feat that every member of the team holds this certification.

Burton said many of the Soldiers left high-paying information technology jobs to deploy.

"You're paid a lot more in the civilian sector for what you do than what the United States Army can pay you," he said. "That's admirable."

B/782 MI BN -- Don't stifle the innovation (cont.)

Continued from page 19

unmotivated to excel. In this environment, the high performers will look around for other things to do, and the Army will lose valuable talent.

It seems to me if we study our rich Army history, we will see commanders that were expected to assume some risk. Conducting proper risk assessment and emplacing mitigation procedures ensures that the benefit has been calculated to be worth the risk. Commanders were not expected to throw caution to the wind, but were expected to be daring and bold. During World War II some commanders were actually expected to fail. Their leaders knew they were not up to the task, and expected them to fail. Not only did they expect them to fail, they expected them to learn from their failures. They put the unfortunate commanders in other positions of less responsibility until they became worthy of more load. This shows that the higher headquarters expected their subordinate leaders to exercise mission command, assume calculated risk, and exercise disciplined initiative.

What We Need In Order to Ensure the Exercise of Disciplined Initiative

Carl von Clausewitz said, "Given the same amount of intelligence, timidity will do a thousand times more damage in war than audacity". More levels of risk assumption and decision making authority need to be delegated down to the mission commander level. This can be defined by higher headquarters, but should have buy in from the company grade leaders that operate where the rubber meets the road. Sure, this may mean more training for the mission commanders. But we need to understand that the mission commander does not operate in a vacuum. He has the EA and the operator with a lot of experience to advise him on the consequences of his decisions in cyber space. They too have a stake in the process and are also held accountable to a certain degree. The members of the team know their jobs and they know their targets very well. Much more so than the higher headquarters that is making the decisions for them. The team, led by the mission commander, knows better than to shut down the entire internet.

In Conclusion - "…the enemy does something unforeseen, there is a new or more serious threat, or a golden opportunity emerges that offers a greater chance of success than the original course of action"

Citing the above quote from ADP 6-0 paragraph 1-59, I cannot list how often on a cyberspace operation that very situation occurs. As cliché as it may sound, the enemy always gets a vote. How do we react when the enemy responds to our actions? Targets of opportunity pop up, but are not on the authorized list. Threats often arise, but instead of combating them we simply leave. If we are to be a lethal cyber force, a combat multiplier to combatant commands, we cannot continue like this. As long as the mission commander meets the higher headquarters intent, and achieves the desired mission end-state, he should have the freedom of action to violently execute as best he sees fit. Our Army mission commanders are some of the best and brightest company grade officers the DoD has to offer. We need to trust them.

HHC/915 CWB -- Building Our Expeditionary Cyber Force (cont.)

Continued from page 27

like taking a puppy to a dog fight. Secretly, you just hope the puppy survives. Thankfully, my Soldiers refuse to let our unit's size or age hamper our success. On the contrary, the members of CWB that attended Saber Junction 19 not only stayed afloat but made waves as they exercised the innovative capabilities of which CWB is capable. As an HHC commander, I consider my primary role to be an enabler. It's my job to make sure that my Soldiers can focus on the mission. This is why my main focus has been standing up all the Army programs that focus on the physical and mental welfare of Soldiers and their families. As a brand new kind of unit, Army Cyber Command is still conducting analysis on the operational and administrative control of our battalion. This means that I've had to do a lot of leg work in determining who – if anyone – is the next level up for these programs. I've spent countless hours visiting offices around the installation learning as much as I can about Soldier and family wellness programs and the role a Commander plays in each the one. From encouraging our Soldiers' participation in Fort Gordon Christmas House, sending Soldiers to

Continued on the next page

Continued from the previous page

training for Additional Duties, and collecting information on medical support programs, I'm investing my time now to buy back precious time when my Soldiers will need these support programs.

The Army has a process for building and staffing its units with the right personnel; however, sometimes the right personnel aren't those who look good on paper. When time is sparse and the operational need is great, the right people are those who are up to the challenge. The right people are those willing to take initiative, learn on the job, and take a few well calculated risks. That's the mentality that is building the Army's newest cyber capability, the Cyber Warfare Battalion. That's the mentality that gets tomorrow's Army built today.

HHC/780 MI BDE -- Mission Command in Cyber (cont.)

Continued from page 28

the cloud it will be hard pressed to find a place where we could not deliver effects.

How do we translate the freedoms of ground forces to mission command in Cyber. First, flip the risk triangle. Currently, we hoard the risk acceptance at the higher levels. Let's examine the full risk profile and reserve the absolutely critical, high risk situations at the higher levels and delegate the rest of the risk down, as far as possible. This requires a better understanding of the domain and the true risk by those at those higher levels, so subject matter experts and feedback from the bottom are critically important. Next, ensure there are clear objectives and commander's intent at every level and major operation. Ensure there are clear and common-sense rules of engagement. Then give more freedom to leaders at all levels to execute against that intent. I ensure you it will grow innovation and breed faster results. Finally, trust in our training and don't bloat it. This trust should come from validation of our teams and the successful accomplishments of the missions conducted so far.

Mission command has been the key to success for ground forces for decades. It has enabled us to be agile and adaptive, staying ahead of our adversary. Let us continue that success in cyberspace.

Cyber program graduate (cont.)

Continued from page 30

processes and find alternatives options to improve them. I spent most of the last five years working as a consultant helping a variety of customers build better software by figuring out how everything fits together, understanding their unique workflows, and developing products to improve both the technical and human aspects of the process."

What assignments and opportunities do you have as a cyber officer?

"There are many opportunities for Cyber officers in the Army. For me, software developer and development team lead are two of the most likely."

What is the most exciting or interesting part of being a commissioned cyber officer?

"To me the most exciting part of being a commissioned cyber officer is being able to do what I am already passionate about in defense of this nation."

Looking into the future, what technologies and skillsets do you predict the Army should be looking to acquire and develop?

"Moving forward in Cyber, I believe the Army should focus on technologies used to secure the tactical edge and build skills used to operate in modern cloud-based computing environments."

What advice do you have for Soldiers or civilians who wish to someday be direct commissioned in the Army?

"There are only two things necessary to direct commission as a Cyber officer; the army will teach you the rest. The first is a desire to serve which will give you the motivation and resiliency to get through the process. The second is a technical skillset to fill a critical gap in the force. These gaps are shrinking and changing as the Army improves its training, but there will always be skills in the private sector that the Army is interested in acquiring through this program."

What's next in your Army career? What are you looking forward to the most as a cyber officer?

"Now that I am finished with BOLC, the next step is to get started at my new unit and start contributing to the fight. The thing I look forward to most is making an impact on the nation's defense through work in the Army's Cyber force."

No losers in SANS NetWars Competition

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

***WASHINGTON** – Soldiers from the Cyber Protection Brigade (CPB), U.S. Army Cyber Command (ARCYBER) teamed up to compete against the top cyber teams in Air Force, Navy, Marines, Coast Guard and National Guard for the 2019 NetWars Services Cup, while other Soldiers, Army and DoD Civilians competed against 178 other champions, individually or in teams of up to 5 players, in the NetWars Tournament of Champions hosted by the SANS Institute, December 15 and 16 in the International Ballroom of the Washington Hilton. (U.S. Army Photos)*

WASHINGTON – Soldiers from the Cyber Protection Brigade (CPB), U.S. Army Cyber Command (ARCYBER) teamed up to compete against the top cyber teams in Air Force, Navy, Marines, Coast Guard and National Guard for the 2019 NetWars Services Cup, while other Soldiers, Army and DoD Civilians competed against 178 other champions, individually or in teams of up to 5 players, in the NetWars Tournament of Champions hosted by the SANS Institute, December 15 and 16 in the International Ballroom of the Washington Hilton.

Ed Skoudis, a SANS fellow and creator of NetWars, said the Tournament of Champions is an invite only event. SANS only invites the people who have won their NetWars events over the last two years and that the game teaches real-world cybersecurity skills – offensive, defensive, analysis, and digital forensics skills.

In the past six years Skoudis has seen a marked improvement in the level of expertise of the U.S. military teams.

"Ten years ago is when we started NetWars, and when we first started NetWars, the U.S. military personnel did o.k., and that's not good when you're doing just o.k.," said Skoudis. "Now, whenever we run a NetWars event, whether it's the Tournament of Champions or anything else, the U.S. military is well represented among the winners. I do think that shows the investment in those skills is paying off, and cyberspace is a dangerous place, and we need our military forces to be ready to defend the country."

In this year's Tournament of Champions two Department of Defense teams placed in the top five – third and fourth place.

Matthew O'Rouke, an Army Civilian with the 782nd Military Intelligence (MI) Battalion (Cyber), was the team captain of Nation_State_Alchemy who placed third. The other team members included: Sgt. Andrew Beat, a cyber operations specialist assigned to the 782nd MI Bn.; Carl Peterson, Chris Maloney, and Neil Klissus, who are DoD Civilians within the U.S. Cyber Command community.

O'Rouke said the cybersecurity and information security training facilitated by SANS is some of the "most well-tailored and practical training given by an organization in this field." He added that NetWars is held at approximately 50 SANS training conferences throughout each year and is included free when attending one of their hosted classes.

"It is always encouraging to see Soldiers and Civilians participate in these events because more often than not they perform incredibly well and above expectations, increasing confidence not just in their skills, but also in their peers they work with every day," said O'Rouke.

Continued on next page

WASHINGTON – *Matthew O'Rouke, Neil Klissus, Carl Peterson, Sgt. Andrew Beat, and Chris Maloney, teamed up to compete against 178 other champions during the individual and team portion of the Core NetWars Tournament hosted by the SANS Institute on December 16.*

Continued from previous page

O'Rouke believes leaders at all levels should recognize competitions like this as another great tool for relevant individual and collective training.

"There are thousands of different ways to improve yourself and others, this is just one example that focuses specifically on the digital battlefield and our cyber work," said O'Rouke. "By doing this, it can either be an opportunity on advanced training for more senior members to share what we know and increase overall team proficiency or it's a great opportunity for junior Soldiers or new Civilians to provide a more hands-on approach to focused and direct individual training. Either way, it's always a good chance to better learn more about the skills of our highly trained team members and strengthen our trust and confidence for future real-world operations."

For Sgt. Andrew Beat, a cyber operations specialist assigned to the 782nd MI Bn., these Capture the Flag (CTF) events give him exposure to a myriad of challenges which will assist him in refining his research and development, and problem solving processes.

"Being able to solve the problem and find the solution is a big part of my job," said Beat. "My leadership will come to me and my colleagues, and say 'we want to be able to do this' and we have to figure out is this technically feasible, is it safe to do so, and can we do it. What requirements, what gaps do we have to be able to do this."

In order to give an idea of what the teams and individuals might face in a SANS NetWars Tournament O'Rouke gave this perspective.

"What we learned were heavy blue (defensive cyber) team tactics deployed in a very dynamic environment. Part of this was out of necessity because one of the teams targeting us had heavily scripted their attack methods so we had to respond manually as we identified and signature the exploit and attack vectors," said O'Rouke. "Within the hour we had signatured and patched/secured the vulnerabilities they were taking advantage of and this resulted in the adversarial team switching to manual targeted attacks; the resulting hours were what could be best described as a 'cyber knife fight'".

The team representing the U.S. Army in the 2019 NetWars Services Cup were Soldiers assigned to the Cyber Protection Brigade, U.S. Army Cyber Command, and included: Capt. Michael Milbank, team captain, Capt. Braxton Musgrove, Chief Warrant Officer 2 (CW2) Michael Edie, CW2 Michael Shue, Warrant Officer Christopher Watson, and Staff Sgt. Buffye Battle.

"Being placed in a contested environment with actual adversaries offers us a chance to test new strategies, enhance our tactics, and rehearse our procedures so that we are more effective and adaptive in real-world scenarios," said Milbank.

Continued on page 49

WASHINGTON – *Capt. Braxton Musgrove, Chief Warrant Officer 2 (CW2) Michael Shue, CW2 Michael Edie, Warrant Officer Christopher Watson, Staff Sgt. Buffye Battle, and team lead (not pictured) Capt. Michael Milbank, Soldiers assigned to the Cyber Protection Brigade, U.S. Amy Cyber Command, represent the U.S. Army at the 2019 NetWars Services Cup on December 16.*

No losers in SANS NetWars (continued)

WASHINGTON – *Roy Luongo, and Aaron Lewis, Army Civilians assigned to the 780th Military Intelligence, U.S. Army Cyber Command, compete against 178 other champions during the individual and team portion of the Core NetWars Tournament hosted by the SANS Institute in the International Ballroom of the Washington Hilton on December 16.*

"Our team is incredibly thankful to SANS for putting together this competition, and thankful to the Army for providing the training and opportunity to allow us to be successful."

While the Army team did not place in the top three – the top three finishers in the Services Cup were the U.S. Air Force, U.S. Navy, and U.S. Coast Guard – Milbank remarked their participation was a great way to improve team cohesion, develop individual technical skills, and also share tactics across the cyber community.

WASHINGTON – *Carl Peterson, a DoD civilian and team member on Nation_State_Alchemy, is competing the SANS Core NetWars Tournament of Champions in the International Ballroom of the Washington Hilton on December 16.*

"The main focus over the next year will be building our own environment similar to what we saw in the competition, employing the techniques we saw other teams using, and practicing and refining our processes," said Milbank.

All of the Soldiers, Army and DoD Civilians remarked that they are always looking for opportunities to improve and hone their skills, and everyone benefits from the exposure.

"You have to continuously broaden your horizons, learn more technology, learn more information systems, more tools to use, because as the environment evolves, we have to evolve with it, otherwise we very quickly become outdated," said Beat. "That's why some people call cyber one of the most hardest domains to lock down because the landscape is always changing, requirements change daily, if not hourly based on what we're using, what the adversary is using, what's the newest technology…what may work one day, might not work the next."

WASHINGTON – *Staff Sgt. Buffye Battle and Warrant Officer Christopher Watson, Soldiers assigned to the Cyber Protection Brigade, U.S. Amy Cyber Command, represented the U.S. Army at the 2019 NetWars Services Cup on December 16.*

1st Annual Presidents Cup

WASHINGTON – The first annual President's Cup Cybersecurity Competition wrapped up on December 12. The competition began in September and drew more than 1,000 individuals and 200 teams. After two qualifying rounds, 10 individual finalists and five team finalists came to the Washington, D.C. area for the final round at the CISA Cybersecurity Lab. The President's Cup is designed to highlight the extraordinary cybersecurity talent in the federal government, and to promote careers in the field.

"The President's Cup Cybersecurity Challenge is just one of the ways we're working to build the nation's cybersecurity workforce – by identifying, highlighting, and rewarding the top talent in government," said CISA Director Christopher Krebs.

The President's Cup was called for in Executive Order 13870, https://www.whitehouse.gov/presidential-actions/executive-order-americas-cybersecurity-workforce/, on America's Cybersecurity Workforce, which the President signed in May.

WASHINGTON – *The winning team, posing for a photo with CISA Director Christopher Krebs (far left), and ARCYBER commander, Lt. Gen. Stephen Fogarty (at right), was composed of (from second left to right), Staff Sgt. Matthew Cundari, Cyber Protection Brigade, Major Josh Rykowski, U.S. Army Cyber Command; Chief Warrant Officer 3 Benjamin Koontz, Defense Information Systems Agency; Sgt. 1st Class Zachary McElroy, CPB, and Chief Warrant Officer 4 Phillip Smith, 781st Military Intelligence (MI) Battalion.*

"The final challenge was two days. The first day was a traditional jeopardy style CTF with 10 questions each worth 1000 points. The questions focused on things like forensics, reverse engineering, covert channel discovery, steganography, and network traffic analysis. The second day of the challenge was a virtual escape room. We were placed in a chemical facility with 10 rooms and had to use the items available to escape. There were computers to compromise, credentials to find, and puzzles to solve," said Smith. (Courtesy Photos)

WASHINGTON – *The team from 782nd MI Battalion was the 2nd place overall team at the President's Cup. from left to right, Chris Krebs, director of CISA; the team: James Hogan, Mike Merrill, Maj. Stephen Hudak, Jeremy Falls, and John Francis; and Lt. Gen. Stephen Fogarty, commanding general ARCYBER).*

WASHINGTON – *Capt. Nolan Miles, assigned to Detachment-Hawaii, 782nd MI Battalion, represented U.S. Army Cyber Command and the Army when he competed in the 2019 President's Cup Cybersecurity Competition and placed 3rd overall in the individual competition.*

780th MI Brigade Holiday Ball

NORTH AUGUSTA, S.C. *-- the 780th Military Intelligence Brigade (Cyber) hosted their 2019 Holiday Ball on December 5 at the Crowne Plaza Hotel. (U.S. Army photos)*

Santa was in the receiving line with the keynote speaker, Brett Goldstein (left), the director of Defense Digital Service, Command Sgt. Major James Krog, the brigade's senior enlisted leader, and Col. Brian Vile, commander of the 780th MI Brigade.

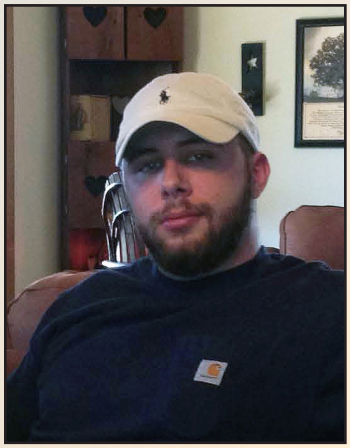
Lest we forget... *The 780th MI Brigade honors our Army traditions by remembering our missing and fallen comrades.*

In his remarks, Brett Goldstein, the keynote speaker, said his organization and others want to help the Soldiers and Army Civilians of the 780th MI Bde., "Some of the things we forget in this room are, for people on the outside, (your mission) is so important, it is so respected, and so critical."

The Brigade recognized the NCO of the Year, Sgt. Kyle Tamraz (center), B Company, 781 MI Battalion, and Spc. Eva Perry, B Company, 782d MI BN, who was not only the Brigade's Soldier of the Year, but the Linguist as well. She couldn't make it this evening -- she was in language training!

Command Sgt. Maj. James Krog (from left) received the Gold St. Isidore Award, and three others received the Bronze Award: Maj. David Hamlin, 1st Sgt. Tammy Cross, and Chief Warrant Officer 2 Jeremy Harris.

In Remembrance of Joshua J. Cothern



Joshua J. Cothern

April, 9 1989 – December 2, 2019

C Company, 782nd Military Intelligence Battalion (Cyber), Fort Gordon, Georgia

Josh was born in Oak Harbor, Washington on April 9, 1989 to his loving parents, Jim and Lisa Cothern. His Family then moved to Slidell, Louisiana, where most of their relatives resided. Josh spent the next three years playing with cousins and being spoiled by relatives—especially grandparents. When Josh was four, his parents moved to Tennessee where his younger brother Cody was born.

Josh was always a very active and outgoing child. He loved playing soccer, basketball, running, going to playgrounds and eating snowballs whenever he visited Louisiana. His love of sports started with T-Ball at five, soccer at six then continued with anything that kept him active. He always had a burning desire to be the best at whatever he did and set high goals for himself. He could and would challenge adults until he got answers to his questions, or until they admitted they didn't know the answer. He was a deep thinker and loved to have fun but mostly, he loved basketball.

Josh graduated from Randleman High School in 2007 where he played point guard on the basketball team. A year later, he surprised everyone by wanting to join the military. He chose to enlist in the United States Air Force in August 2008 working in Intelligence. After completing Basic Training in San Antonio and school in San Angelo, Texas he was sent to Anchorage, Alaska as his first duty station. While there, he continued his love of sports while enjoying snowboarding and fishing before

deployment to Afghanistan. Josh returned home just prior to the birth of his daughter, Reagan Lane, the light of his life.

After his enlistment was complete, Josh worked as a contractor in Maryland before he and Reagan moved to Augusta, Georgia where he was employed as a Civilian with the Department of the Army. Josh and his little shadow Reagan, enjoyed every spare minute together. He was a wonderful father and devoted himself to Reagan. She was always at his side, helping him fix his truck, going to a rodeo or working on the farm.

Josh is survived by his daughter, Reagan; his father and mother, Jim and Lisa Cothern; his brother Cody, and many close relatives, Family and friends.

FREDERICK, Md. - Soldiers from the 780th Military Intelligence Brigade (Cyber), Soldiers from the medical branch, and a team from the U.S. Naval Academy, supported a Maryland STEM (science, technology, engineering and math) Festival event to encourage teen girls to consider a career in the fields of STEM at Frederick High School on October 24. (U.S. Army photo)