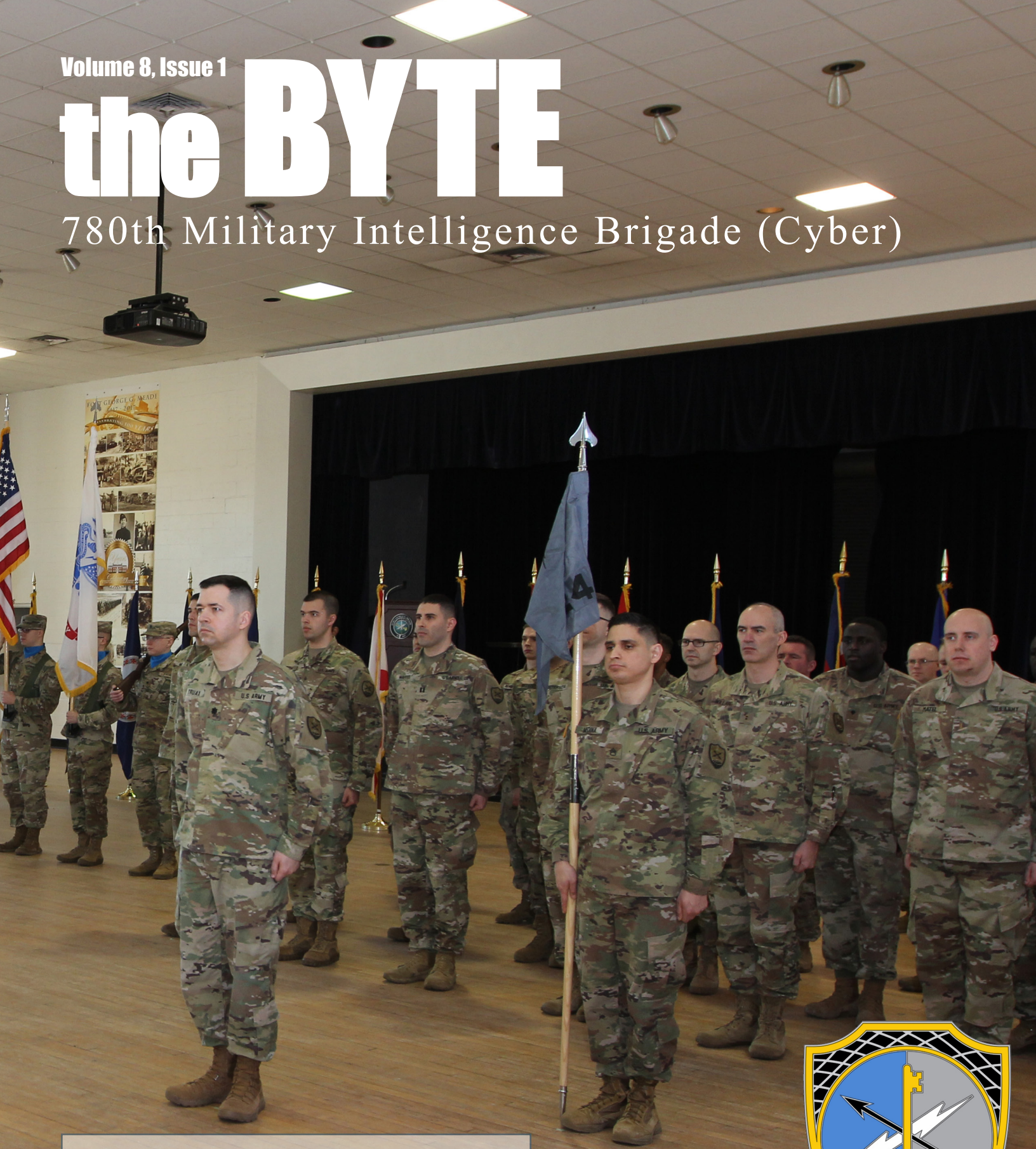
Volume 8, Issue 1

the BYTE

780th Military Intelligence Brigade (Cyber)



* Army National Guard transitions Task Force mission
* The Praetorian Best Warriors are...

Mutual Trust and Commander's Intent

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 BDE and their Families.

Opinions expressed herein do not necessarily represent those of 780th MI BDE 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 graphics contained within the BYTE were created by the Brigade public affairs officer (PAO), Steven Stover, or the Brigade Graphic Designer, Quintin Wilcox, unless otherwise stated.

Send articles, photographs or story ideas to the 780th MI BDE PAO at steven.p.stover.civ@mail.mil, or mail to 320 Chamberlin Avenue, Fort George G. Meade, MD 20755.

For additional information, call (301) 833-6430.

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 GEORGE G. MEADE, Md. *– The 780th Military Intelligence Brigade (Cyber), hosted a transition of authority ceremony at McGill Training Center on February 21, between two Army National Guard formations whereby one cyber battalion transitioned with another to continue the Task Force Echo cyberspace mission in support of U.S. Cyber Command. (US Army Photo)*

Features

Articles

From the Editor

The theme for this issue of the BYTE is *"Mutual Trust and Commander's Intent."*

In accordance with ADP 6-0 Mission Command, *"mutual trust is shared confidence among commanders, subordinates, and partners. Effective commanders build cohesive teams in an environment of mutual trust." ... "The commander's intent is a clear and concise expression of the purpose of the operation and the desired military end state that supports mission command, provides focus to the staff, and helps subordinate and supporting commanders act to achieve the commander's desired results without further orders, even when the operation does not unfold as planned."* (JP 3-0)

Although intentionally a broad topic, the command was not looking for definitions of mutual trust and/or commander's intent, but rather a thought-provoking article using the principles of Mission Command and how they apply to the Cyber and Information Warfare Enterprise.

And while we cannot publicly name our adversaries, discuss named operations, or specifically identify our partners, we are the only offensive cyberspace operations brigade in the U.S. Army and we actively conduct cybersecurity operations to deliver effects in support of Army and Joint requirements.

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

v/r,
Steve Stover

Public Affairs Officer
780th MI Brigade
Editor, the BYTE

'80MIB QRCode.png

Information Warfare

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

Praetorians:

The nation relies upon the capabilities we provide to deter, and when directed, defeat our adversaries in and through cyberspace. We are part of the thin, gray line between competition and conflict.

There are sparingly few non-kinetic options our commanders can leverage to influence our enemies; offensive cyber is one of those tools. If we are successful, our nation remains in competition short of conflict. If we fail, our military may be forced to resort to kinetic action to defeat our adversaries. The costs of our successes are trivial compared with the price of failure.

However, effects delivery in cyberspace is not the only tool available in the competition phase. To the contrary, one of the most powerful uses of the Brigade is to deliver effects through cyberspace, specifically targeting our adversaries via the information environment. This use of cyber is a critical component of information warfare – leveraging the information environment to gain the advantage over our enemies. Although manipulating and shaping the information environment is an age-old tool, the creation of cyberspace has opened up new and innovative ways to influence our adversaries. As professional Soldiers and Civilians, we need to be prepared to win the information fight.

Information warfare is, and has always been, one of the most powerful tools in conflict for two reasons. First, once a conflict has begun there are only two paths to victory: change your enemy's mind, or kill them. Second, information warfare, like effects delivered in cyberspace, can be used to change our adversary's calculus on whether or not to enter into conflict.

Most wars end when one side changes their mind about the costs of continuing the conflict. However, one cannot conflate strategic victory with tactical success; winning on the battlefield is not a guarantee that the other side will submit. History is full of examples where a nation of great power, despite tactical successes and overwhelming resources, lost their will to fight.

During the Second Punic War, the Carthaginian General Hannibal was defeated not by pitched battles, but rather by a Roman war of attrition. Without a doubt, Hannibal was a master of tactics, handily defeating the Romans in battle after battle. Realizing he had little hope of removing the Carthaginians from Italy through massive battles, the Roman Dictator Fabius instead denied the Carthaginians victories on the battlefield by attacking Hannibal's supply lines and morale. Although initially relieved of his leadership role by politicians looking for quick, tactical wins, Fabius was eventually reinstated and "Fabian Strategy" – attriting your enemy over time to change their mind – became part of military history.

During the American Revolution, George Washington earned the nickname the "American Fabius" for his employment of the tactic against the British. Unfortunately for the United States, recent conflicts in Vietnam, Iraq, and Afghanistan demonstrate that we too are vulnerable to this tactic, whether used by design or happenstance.

The alternative path to victory is killing until everyone that opposes you is dead. One famous historical example of winning through killing was the Third Punic War, the last fought between the Romans and the Carthaginians. In this war, the Romans achieved final victory by reducing the city of Carthage to rubble and ash, enslaving its people, and (in legend) plowing salt into the ground to prevent their civilization from ever posing a threat again.

This method of war is costly, and the actions required to win via killing may put us at odds with our norms and values. This method is also rarely successful.

In practical execution, armed conflict starts with killing in the physical domains and ends in the cognitive domain. Killing continues as necessary until those remaining (on one side or both sides) lose the will to continue fighting; an end is negotiated or one side surrenders. Both World Wars used this model and victory came at a massive cost in human lives. But the killing itself didn't achieve victory –

instead, those still alive changed their minds about the costs associated with continuing conflict. Every bullet we fired to achieve victory sent a message.

This is why information warfare is a critical component in modern warfare – if waged successfully, it will erode our adversary's will to fight, thereby shortening conflict, saving lives, and ensuring our objectives are met.

But where information warfare is most valuable is in preventing conflict. The decision to enter into armed conflict is based on a complicated calculus of cost and benefit. Leaders and nations must consider the diplomatic, military, political, and fiscal costs of conflict, both at home and abroad. The benefit of engaging in armed conflict must outweigh the costs. For democracies, these conditions rarely exist.

Our adversaries understand this and will often use our peaceful tendencies against us. Russian Information Confrontation is predicated on creating a cloud of cognitive uncertainty to shroud decisive action. As seen in Russia's actions in Crimea, it is possible to shape the information environment in such a way as to suppress a potential opponent's desire to fight. The Russians successfully suppressed information that would have bolstered our will to confront them, while at the same time sowing disinformation to make the media and politicians question the facts that were known. The Russians are not alone in manipulating the information environment; China has a sustained campaign to influence U.S. media outlets, academia, and other critical players in the information environment.

As the Army's only offensive cyberspace operations brigade, we play a critical role in information warfare. In the past, the information fight was fought through radio stations, leaflet drops, printed media, television ad buys, and press conferences. The influence battles of the future will be fought online; social media is a battlefield and our adversaries will reinforce their efforts there through disinformation disguised as fact.

As cyber leaders, we must understand and embrace information warfare. Cyber-enabled information warfare allows us to influence our adversaries at every level – strategic, operational, and tactical. We must appreciate that sometimes the public reaction is more powerful and damaging to our adversaries than the tactical effect. Consider Doolittle's raid on Japan early in World War II. By any measure, the tactical impact was minimal. However, the strategic impact was massive. Not only were the Japanese forced to use precious resources to defend the homeland, his raid gave hope and energy to a nation still reeling from the massive U.S. defeat at Pearl Harbor.

When directed, our efforts to deny, degrade, and disrupt our enemy's information activities in cyberspace must ensure the ability of democracies to make decisions based on fact. At the same time, we must target our adversary's decision makers while disrupting their ability to sow disinformation to their own populace. Our enabling activities in cyberspace and the information environment will allow the U.S. to degrade our adversary's will to fight by disrupting their cost-benefit calculus.

Should conflict occur, information warfare will deny our adversary clear wins and situational understanding. Like Fabius, our Brigade can attrit our adversaries without direct contact; we can change their mind through our actions in the information environment.

The key to successful information warfare is the same as the key to successful cyberspace operations: well-trained, agile, adaptive, and opportunistic forces with leaders who exercise mission command. Only by empowering our junior leaders on the frontlines of information operations will we see anything more than limited and episodic success. The pace of evolution in the other domains of warfare is measured in years, decades, and centuries. Information warfare – like cyberspace operations – requires us to adapt our tools, techniques, and actions in minutes and hours.

Cyberspace has become the primary battlefield for information warfare, and will remain so for the foreseeable future. As we continue to mature cyberspace operations, all leaders must recognize the importance of the convergence of the newest domain with the oldest and most important battlefield - the human mind. Just as our predecessors integrated and utilized siege machines, gunpowder, and air power into warfare, we must be just as innovative and leverage our exceptional technical skills to fight and win information warfare.

PRAETORIAN 6

"Strength and Honor"

Mutual Trust & Commander's Intent

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

This quarter's topic of mutual trust and commander's intent has been an important part of my life for the last 25 plus years. They are two distinct principles of Mission Command, and yet they go hand-in-hand and are proportional with each other. It is possible to have one without the other, but this is not optimum and will likely lead to mission failure.

One can have all the trust in the world, but without understanding and meeting the commander's intent, mission success is improbable. On the other hand, one may have complete understanding of the commander's intent, but lack of trust could lead to second guessing, micromanagement, or mission creep and potentially create conflict where the recipient may no longer care about the commander's intent because he or she is not able to execute appropriately. Building cohesive teams through mutual trust and understanding the commander's intent are both necessary to fully meet the objectives of the mission

How a commander conveyed his or her intent has dramatically changed over the years with the improvements in technology. Now this may amuse some, but when I first joined the Army, the internet and cell phones did not exist and computers were few and far between. The commander conveyed intent by receiving an order, conducting an orders brief, and receiving a back brief. I may or may not have received a copy of the order. If I did, I had a short time to digest the information in the order before moving to a designated location to receive an orders brief from the commander. After receiving my the brief, I returned to my platoon, squad, or team and read the information from the notes I had taken to my Soldiers. Together, we identified the tasks we were to accomplish and when we were to accomplish them; conducted, at the minimum, a map reconnaissance of the location or locations we were to go; identified any friendly or enemy personnel or information that may impact our mission; and performed a slew of other tasks that were necessary to prepare for our mission. At the designated time, I returned to the command area and conducted a back brief to the commander. This was done using a sand table or map. At the back brief, I verbally and graphically briefed the commander what my mission was, by phase, and how I was going to accomplish the mission based on the order. I had to know the mission inside and out, take notes, and gain clarity, to fully prepare for and execute my assigned mission. The better the back brief, the more trust the commander had in my meeting his or her intent and accomplishing the mission. We had radios for communication, but that was the only method of communications we had. The commander had to trust that I would use the intent to accomplish the mission and I had to understand that if I didn't, there would be consequences.

Today, the concepts are still the same, but technological improvements have made it easier to receive the order, conduct an orders brief, and perform a back brief. Colocation with leadership is no longer necessary as these can be conducted via VTC or telephone. Power Point and mapping software make conducting the back brief easier as everything can be performed on a computer.

Continued on the next page

Continued from the previous page

Everyone that requires a copy of the order can get a copy of the order via email, a shared drive, or an online portal, each of which can be referenced at any time.

In many ways, this is easier, but not necessarily better and there is a much greater reliance on mutual trust. Without face-to-face interaction, trust is necessary to ensure complete understanding of the commander's intent and any subtle nuances that may not be clearly articulated in electronic communications. However, it is also easier for the commander to see the action on the battlefield and adjust as necessary through technological advances such as improved battlefield tracking systems, imagery, and unmanned aerial systems. This makes battle tracking easier, but does not lessen the need for mutual trust and clear understanding of the commander's intent.

Leaders on the battlefield must have the trust of their commander in order to be empowered to exercise disciplined initiative to accomplish the mission. While mutual trust is a vital component to meeting the commander's intent and accomplishing the mission, it is also a key aspect to being a leader in the Army. Leaders must have the trust of their subordinates in order to build effective teams. Subordinates must trust that their leaders have their best interest in mind and will not do anything to harm them. A leader that does not have the trust of his or her subordinate is not the leader. Without this trust and belief, there is no team, just a group of individuals performing day to day activities.

What I learned over the years is that sometimes a leader has to explain *'Why'* to a subordinate. Today's Soldiers are connected to everything via social media, the internet, cell phones, and a multitude of other forms of technology. They may not understand the reason a decision is made without someone explaining why. This should not be taken in a negative light as it isn't a negative thing. The thirst for knowledge today is greater than ever and that includes the need at times to explain the *'Why'* of something. It is also a method to build greater trust in the team and reinforces that the leader is there to take care of the Soldier and or Civilian while also accomplishing the mission. Trust is key to a subordinate to leader relationship and must go both ways. Leaders must trust that their subordinates will accomplish the tasks assigned to them without fail. A key concept is *'Trust but verify.'* This means ensure the task is accomplished, but do not micromanage it. Micromanagement only destroys trust. As long as there are leaders and subordinates, regardless of the type of organization, mutual trust will be required to build the team and accomplish the assigned mission.

As this will my final Byte article as the Brigade Command Sergeant Major, I want to say it has been a great pleasure serving with you and to thank you for all of your support over the last two and a half years. I am grateful that the Army saw fit to give me this assignment as the last one of my Army career. I could not have asked for a better unit or a better group of people to work with. Thank you for everything that you do and I hope to work with you all again in the future. I have the utmost respect for you and wish you continued success in everything you do. Thank you again for everything.

PRAETORIAN 7

"Strength and Honor"

A Nibble on Mutual Trust and Commander's Intent

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

Do you remember what you wanted to be when you grew up? If you are like me, you likely listed something entirely different than what you are currently doing. I wanted to work for the Forest Service or to own a ranch, neither of which have come to fruition – yet. I remembered thinking that the Army was a last resort option if all other attempts to get my adult life started were to fail. No need to elaborate, but here I am, all the better for having made the decision that I did to serve.

Why do I bring this up? To dig into some of my thought processes and influences as a junior Soldier and to draw some conclusions that may be of use as we struggle with the ebb and flow of personnel in and out of the brigade.

As a young Soldier, I considered the Army a job. Despite every first sergeant and command sergeant major telling me that the Army was a career and profession, I still looked at the Army as a job. The reason for this was that I wasn't sure that being a Soldier was what I wanted to do for a living. It was a means to an end; namely to acquire money for college that would launch my career outside of the Army in exchange for a four-year term of service.

This was a fair deal and I was happy for the opportunity. Over time, I learned that the Army valued my service and was willing to provide more opportunity by way of promotion, training, and assignments for an additional service commitment. Having this knowledge, I leveraged multiple three-year reenlistments that minimized my commitment while affording me an opportunity to improve my promotion potential and marketability for when I exited the military. It wasn't until I had reached eight years of service that I made a decision that the Army was the career that I would pursue until I was retirement eligible.

The chart in *figure 1* is my unscientific observation of a Soldier's transition path from job to career-mindedness. While a deeper study would produce more fidelity, I think the timeline and thought processes are generally accurate for the majority of those who join the Army at a young age.

While the decision to make the Army a career was a personal process, the following factors were major contributors that made it much easier to do so:

1. Competent leaders who balanced operational objectives with administrative requirements, were engaged with the mission, and provided clear intent
    - This played an important role in my decision process; while not every assignment was ideal, quality leadership was the driving factor that outweighed negative aspects that would have otherwise deterred my decision
    - I wanted to emulate competent leaders who exhibited technical and tactical excellence within the mission
    - These leaders developed mutual trust that flowed horizontally and vertically throughout their command by being mindful of the needs and stresses of their force and working to ensure Soldier needs were met in a timely and efficient manner
    - Additionally, these leaders established clear goals for the unit to accomplish, making it easier for the team to focus energy and resources on things that mattered (they minimized wasted energy and effort)
2. Determination to improve my technical competence through resident and on-the-job training
    - I recognized the value of my assigned mission and was driven to develop a depth of skill that increased my ability to perform at a high level which, in turn, improved my promotion potential and marketability

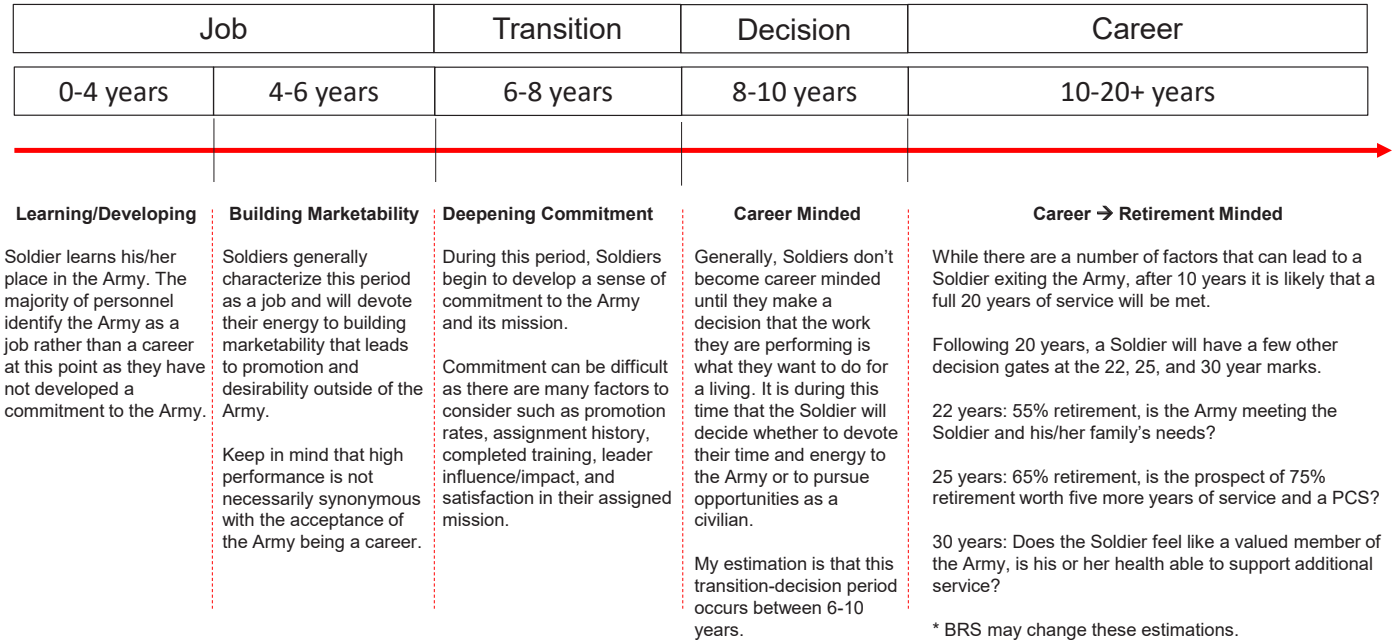


Figure 1: Key phases in transition from job-minded to career-mindedness

- Employing acquired skills in an operational environment improved my competency and built a deeper sense of value and purpose in the work that I was performing

3. The Army provided a means to attain and employ these skills in a stable/predictable manner
   - Leader-facilitated key assignments widened my breadth of experience and ensured I was integrated into the mission as quickly as possible
   - Leadership modified operational schedules and administrative requirements in a manner that lessened stress upon the team while still meeting requirements
   - Stability and predictability throughout an assignment were also significant factors that encouraged me to pursue the Army as a career
4. Being considered a valued member of the team
   - Leadership was involved and committed to the mission at hand – the mission mattered to the whole team, from the Private to the General
   - I was and saw others being trusted with important tasks across a range of strategic and tactical missions
   - Recognition of contributions to the mission, unit, and team encouraged me and my teammates to push the boundaries of our capabilities and to improve the mission function and outputs
5. Reenlistment and incentive options that facilitated additional training and assignment choices and empowered soldiers to become active in their career progression.
   - Early-on I maintained some control by limiting my reenlistments to the smallest increment possible, using them to negotiate for training and assignments
   - Empowerment continued after deciding to pursue the Army as a career as I had learned portions of the Army assignment and training processes, making it easier to navigate the system to attain assignments that deepened my experience
   - Soldiers who are empowered become active participants in their assignments, training and the mission which creates an environment that facilitates career-mindedness

Continued on page 45

Pedaling Faster

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

Vanguard, visiting your workspaces in the last few weeks has left me in awe. The New Year is getting busy and we have responded by getting after it! I wanted to take a moment to summarize my thoughts on mutual trust, commander's intent, and the framework in which we operate.

As a parent, how long would you tell your 5-year-old to "just pedal faster" on her tricycle before it becomes apparent that the only way for her to get to the neighbor's house more quickly is with a bicycle?

Whether we are talking about NASCAR stock cars or growing grapes for wine, a system's true performance becomes fully understood over time. At this point, "just pedaling faster" might yield an improvement but nothing new or different.

Our system is not as simple as a kid on a tricycle. Our operational speed is not a function of "pedaling" but of our personnel and how we organize ourselves; our policies, training, and TTPs (tactics, techniques and procedures); our culture, norms, and expectations; and the authorities and rules that we follow.

What does this have to do with commander's intent?

The 781st is in the effects business. If you are on a team, my intent is that you produce these effects. Our focus must be relentless. Calm, measured, and smart, but still relentless.

Let's talk about encouraging a system based on mutual trust.

Your same 5-year-old falls off their tricycle. You happen to live in a hypothetical city where there are no urgent care facilities, no emergency rooms, and no first responders. In this city there is only one hospital -- a teaching hospital focused on training medical students. When you take your child to this hospital, the care that she receives seems like the byproduct of a system focused somewhere else. You look at this sophisticated, expensive hospital in dismay. It is busy doing stuff, but not stuff that the city needs.

I will leave you with this thought: if you were the mayor of this city, what would you do? What one metric would you start measuring to focus everyone on the bottom line?

My door is always open. Stop by and let me know how we can build our faster bike. I trust you and I will empower us. We got this!

VANGUARD 6

"Vanguard...When Others Cannot!"

FORT GEORGE G. MEADE, Md. *– Capt. Stephen Hart, the outgoing commander of C Company (Conquerors), 781st Military Intelligence Battalion (Cyber), relinquished his command authority to Capt. Matthew Satterthwaite, in a change of command ceremony hosted by Lt. Col. Nadine Nally, commander of the 781st MI Battalion, at the McGill Training Center Ballroom, Mar. 3. (U.S. Army Photo)*

"Ready, Responsive, Resilient"

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

Parade rest. Stand at Ease. Rest. The first thing that most leaders in the Army sacrifice for the mission, rest. From Basic Training to Elite Leadership schools, every Soldier learns to push the limits of their sleep and rest to accomplish the mission. Yet in the same breath the Army created the performance triad; nutrition, fitness, and sleep.

Which is it?

I subscribe to the 'sharpen the axe' mentality. Every Soldier and Civilian needs the time to be able to decompress so that they can properly attack the mission each and every day. The "rest" may not be every day but needs to occur to prevent burnout. The Army has gone to great lengths to ensure Soldiers have the proper amount of rest before missions, especially when flying multi-million-dollar equipment. Why, then, don't multi-million-dollar trained Soldiers and Civilians using multi-million-dollar equipment have the same requirements?

I have charged my battalion from the beginning with being "Ready, Responsive, Resilient". The resilient aspect tends to be one aspect that the Army does not train. It is easy to train readiness. Train and master your job. Training responsiveness comes just as easy. Execute on short notice with a limited window. We accomplish all of these on a regular basis with task, conditions, and standards. But what are the tasks, conditions, and standards for resiliency? This is up to the individual and team to ensure that Soldiers and Civilians can work at their peak.

If we are going to build our teams with mutual trust then we need to learn the limits of our crews and teams. In the previous issue, I wrote about being deployed in place. It is exceptionally difficult to balance this mentality and acknowledge that you need a break. "My team is firing today; I need to be there." I argue that we are not weak to take time off. Instead, we are improving our team through improved mental functioning. My team will trust my actions more with greater clarity in my decision making, and they will function better with greater rest.

While eight hours of rest might be a pipe dream for most of us, we can acknowledge that time away from the problem can help improve our metal capacity. Recognizing this, we are beginning to implement our own holistic crew rest. We cannot reduce many of the activities that you need to do throughout the day: drive to work, eat, 350-1 training, PT, shower (maybe?). But what we can do is maximize the time that you have to rest. While tracking this will initially be cumbersome for leadership, it will increase their ability to trust in your decision-making and allow you more independent freedom.

With this program, the 782d will lead the way. Each and every member will have the time to refocus both mentally and physically. Our leaders have begun tracking the rest and utility of our operators to ensure that our most stressed positions remains capable. We are confident that this will increase the readiness and lethality of the crew, team, and battalion as a whole. Given this top priority we expect that our results will spread across the Cyber Mission Force!

"Cyber Legion...Silent Victory!"

Mutual trust and the shared understanding

By Lt. Col. Matt Davis, commander, 915th Cyber Warfare Battalion

In the quest for the secrets of military success, we often overlook the human factor. Napoleon Bonaparte's greatest victories during the Napoleonic Wars (1803-1815) were due to a variety of reasons: The ability of his Grand Armee to outmaneuver its enemies, better organization and logistics, innovative artillery employment and doctrine. For example, while traditional European militaries of the time deployed their armies in mass, Napoleon organized his forces into smaller, more versatile Corps d'Armee. Moving and sustaining these smaller formations significantly improved the maneuverability of Napoleon's Grand Armee, allowing his army to adapt and maneuver much faster. In fact, vestiges of the Corps d'Armee system pervade most modern armies of the world even today. But while the organizational structure played a role, there is a critical human factor beyond the force design that proved vital to Napoleon's success: Trust. The mutual trust and the shared understanding that Napoleon had with his subordinate Corps commanders frequently proved the deciding factor in both campaigns and battles.

Napoleon placed great trust in his Corps commanders and usually allotted them the freedom of action required to accomplish their tasks. But his Corps commanders also placed great trust in the understanding that Napoleon's guidance to their formation was part of a larger plan, even if they weren't fully knowledgeable on all the details. This is the fundamental trade in trust between commanders at echelon: Higher echelon commanders must trust lower echelon by providing them room to make their own decisions, but lower echelon commanders must trust that they may not always have all the information or the complete picture. The concept of mutual trust is pretty straightforward, but the practice of mutual trust is much more subtle. Mutual trust is

Continued on the next page

François Gérard - L'Histoire par l'image [1], digital version produced by Agence photographique de la Réunion des musées nationaux.

Continued from the previous page

not something that leaders and subordinates gain instantaneously. Reputation and first impressions can affect how subordinates and leaders view each other initially; however, those types of perceptions only survive initial contact. It takes time to build a team that has a common approach to operations and speaks a common operational language. Ultimately, it takes time to build mutual trust up and down a chain of command.

The mutual trust built between Napoleon and his Corp commanders had shared understanding as its basis. Without this foundation, building trust in ambiguous circumstances is far more difficult. His Corps commanders understood not only his specific guidance to their specific formation, but also shared understanding of his strategic objectives and goals, which allowed them to exercise mission command with the confidence that their maneuvers were within Napoleon's broad guidance. For instance, at the Battle of Austerlitz, Napoleon's intended to draw troops away from the Allied center in order to facilitate a direct assault that would break their line and win a decisive advantage. Napoleon had specified which Corps would lead that assault, and general guidance to the others, but not specific maneuvers. All of his Corps commanders shared this understanding of his intended maneuver, thus allowing them to maneuver their formation with confidence knowing that the pre-designated assault corps would launch at the right time.

Although success is typically attributed to the leaders of an organization, it is the mutual trust and shared understanding between everyone, not just commanders, that creates a resilient and adaptable organization. There are many challenges that come with the activation of a battalion created to provide Information Warfare support to echelons Corps and below. Beyond the typical challenges associated with building any military unit, there are several other unique challenges that come with building a unit unlike any other in the Army. This includes developing TTPs (tactics, techniques, and procedures) for a unique mission set, creating an efficient and effective command and control structure that enables integration with the different Army Service Component Commands, developing individual and collective training, and defining future capabilities and equipment requirements. Yet, the same lessons learned illustrated by Napoleon and his Corps commanders provides our battalion a blueprint for conquering vast and disparate challenges in an efficient way.

Despite the obvious challenges, this battalion deployed a fully equipped and trained team to the Joint Multinational Readiness Center, the Europe-based Combat Training Center (CTC), the National Training Center at Fort Irwin, Calif., and on our first OCONUS (outside the continental U.S.) operations; all done in the span of nine months. How did this happen? The answer is simple: The 915th Cyber Warfare Battalion (CWB) is comprised of great Soldiers who are aggressive, innovative, and exercise disciplined initiative on a daily basis. But what makes these accomplishments achievable is a shared understanding and mutual trust in our fellow Soldiers.

The 915th CWB engages with leaders all over the globe to discuss mission opportunities and integration. The majority of these interactions don't happen at the Battalion Command level. The CWB's credibility with Army formations is built and earned by our operators and staff as they engage with their counterparts. In the nine months of 915th CWB's existence, leaders throughout the battalion have shown that given the a little guidance and a high degree of trust, they can achieve exceptional results.

I will not go as far as to say that our unit has achieved complete shared understanding for conducting expeditionary information warfare: We are still learning every day. But while we do not have every answer, we do have a shared understanding of the mission: Bring information warfare capabilities in support of Army requirements. Thanks to the outstanding Soldiers, NCOs, Warrant Officers, and Officers of the 915th, though, we're well on our way.

HARBINGER 6

"Take Everything...Leave Nothing!"

Army National Guard transitions cyber task

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

FORT GEORGE G. MEADE, Md. *– Army National Guard Soldiers assigned to the 124th Cyber Protection Battalion participate in a ceremony to mark their deployment as the fourth iteration of Task Force Echo in support of U.S. Cyber Command. The battalion's cyber warriors hail from Arkansas, Maryland, Missouri, Nebraska, Virginia and Utah. TFE IV is commanded by Lt. Col John Truax, commander of the 124th CPB, with Command Sgt. Maj. Timothy Hawley as the senior enlisted leader. (U.S. Army Photos)*

FORT GEORGE G. MEADE, Md. -- The 780th Military Intelligence Brigade (Cyber) hosted a ceremony between two Army National Guard battalions to transfer the Task Force Echo cyberspace mission, at Fort George G. Meade, Md., Feb. 21, 2020.

The ceremony marked the end of a 15-month deployment supporting U.S. Cyber Command (USCYBERCOM) for the Soldiers of the 126th Cyber Protection Battalion, who handed the task force mission to the 124th CPB during the event.

The members of the 124th hail from Arkansas, Maryland, Missouri, Nebraska, Virginia and Utah, while the 126th is comprised of Soldiers from Alabama, Colorado, Connecticut, Kentucky, Maine, Massachusetts, New Hampshire, North Dakota, South Dakota, Tennessee, Utah and Vermont.

Col. Brian Vile, commander of the 780th, served as host and featured speaker for the ceremony.

"The Soldiers before you today are the warriors of the 21st century, and they bring skills and expertise that are changing the face of modern warfare," Vile said of the two battalions. "Their skillful execution of their technically demanding tasks underpins both USCYBERCOM's and the brigade's ability to perform their assigned missions."

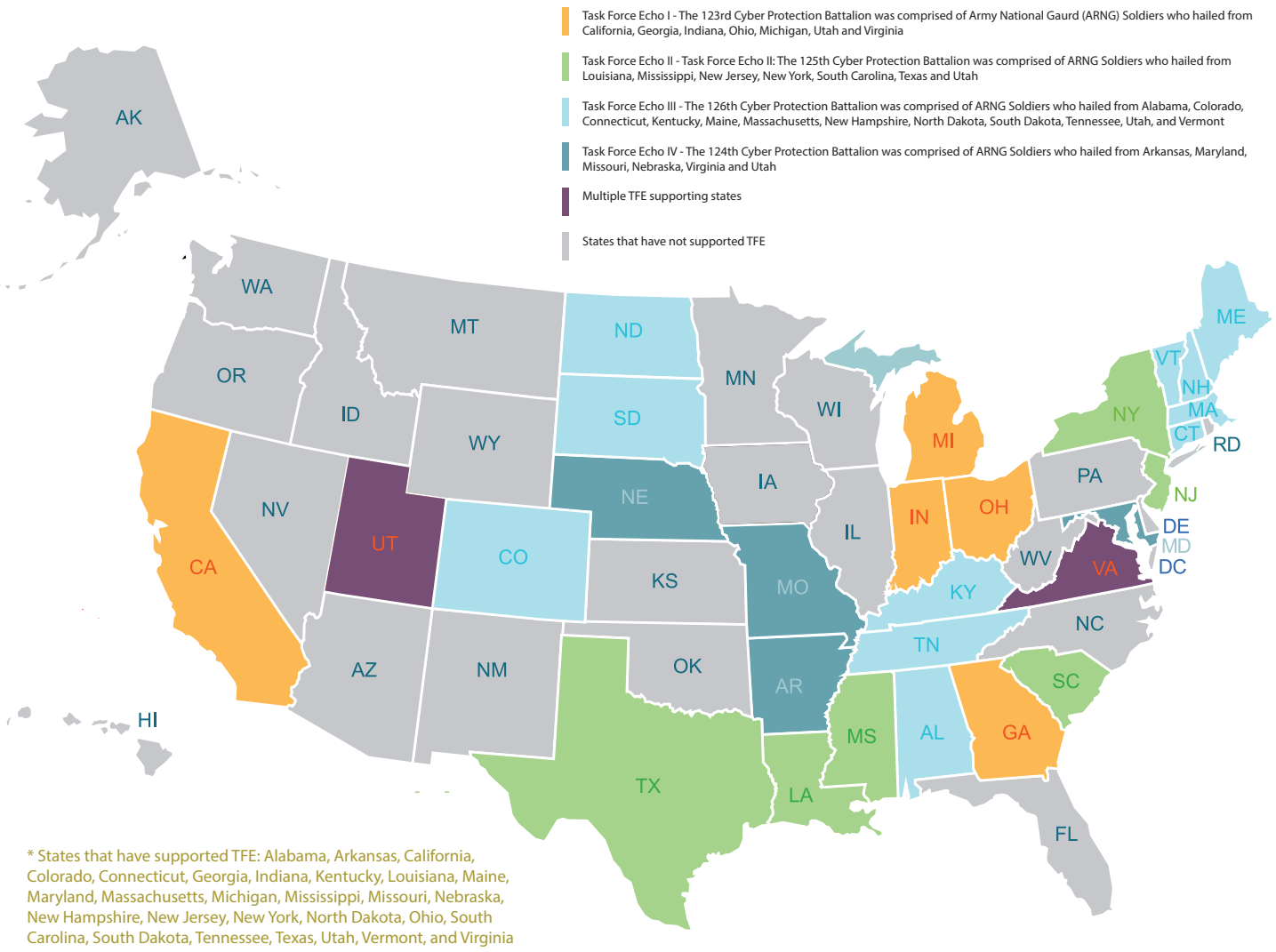
"The decision to utilize the dedicated, experienced, and technically skilled members of the Guard in this capacity clearly demonstrates the integral role the National Guard plays in the defense of our nation," he added. "What is less obvious is that the unique skills and viewpoints they bring to the fight are the critical catalyst that ensures continued momentum from potential to demonstrated capability."

Lt. Gen. Stephen G. Fogarty, commander of Army Cyber Command (ARCYBER), spoke with the Soldiers of the 126th prior to the ceremony and thanked them for their service.

"You are vital to our ability to actually operate," Fogarty said. "What you do is very complex and very critical. What was especially noteworthy for this

Continued on the next page

force mission



* States that have supported TFE: Alabama, Arkansas, California, Colorado, Connecticut, Georgia, Indiana, Kentucky, Louisiana, Maine, Maryland, Massachusetts, Michigan, Mississippi, Missouri, Nebraska, New Hampshire, New Jersey, New York, North Dakota, Ohio, South Carolina, South Dakota, Tennessee, Texas, Utah, Vermont, and Virginia

Continued from the previous page

rotation was that you represented 12 states and came together so brilliantly to not only get the job done, but to make so many great improvements to our core systems and processes."

In the past year three years, more than 450 Army National Guard Soldiers have been assigned to the task force, working alongside the 780th to conduct cyberspace operations in support of USCYBERCOM and the Cyber National Mission Force. The task force is aligned under the 780th, which falls under the operational control of ARCYBER.

Task Force Echo also provides an opportunity for states to send Soldiers to Fort Meade to get certified and receive the education and experience they need to get Army National Guard Cyber Protection Teams to their initial operating capacity and full operational capacity. Task force members return to their home stations with increased skills and with hands-on experience, giving states added capabilities to support their missions.

HHC/781st MI BN Change of Command

FORT GEORGE G. MEADE, Md. *– Capt. Tarama Rainford, the outgoing commander of the Headquarters & Headquarters Company, 781st Military Intelligence Battalion (Cyber), relinquished her command authority to Capt. Tore' Girty, in a change of command ceremony hosted by Lt. Col. Nadine Nally, commander of the 781st MI Battalion, at the Potomac Place Community Center, Feb. 13. (U.S. Army Photos)*

Revisiting Scientific Management

By 1st Lt. Stephen Park, executive officer, A Company, 781st Military Intelligence Battalion (Cyber)

Frederick Winslow Taylor, the father of Industrial Engineering, left a legacy that is profoundly felt in our organizations today. A mechanical engineer by trade, Taylor was obsessed with optimizing efficiency, particularly in management. His book, "The Principles of Scientific Management," is largely considered the single most influential management book of the past century; it attempted to apply 'science' to management.

When consulting factory owners, Taylor reduced every job to its most granular elements. For example, someone installing the engine in a car did not need to understand how an engine works, let alone all of the components of a car; all they would need to know is what bolt they were assigned to tighten. Workers were given instruction cards that prescribed detailed directions for workers to follow, thus removing craftsmanship and skill from the process. The advantage is clear: incredible gains in productivity. The amount of time it took to manufacture a car was reduced from 12.5 hours to just 93 minutes; however, standardization meant that workers were reduced to repetitive and monotonous tasks. There was no need for management to invest in, and develop their workers beyond training them for their basic function. In his own words, *"I have you [workers] for your strength... we have others [managers] paid for thinking."*

This model is the antithesis of the Army's philosophy of mission command. The U.S. military employed many of Taylor's ideas, but while the pursuit of efficiency – getting the most with the least – was undoubtedly central to the success of our military in the twentieth century, is it still viable today?

Today's world is dynamic and increasingly more complex, where organizational hierarchies are not as clear-cut as the traditional model espoused by Taylor. The vast majority of the U.S. military follows traditional formations (i.e. Platoon, Company, Battalion, Brigade, etc.). While the 780th Military Intelligence Brigade (Cyber) follows this model for administrative purposes, our operational formation looks altogether different: the current organizational hierarchy requires less science and more management. Soldiers engaged in cyberwarfare do not share the well-developed SOPs or the decades of experience conducting operations that other branches have. To complicate the situation, the laws and policies governing cyberspace are not yet fully developed.

The success of the Cyber Mission Force requires a radical transformation from the traditional hierarchies of the past. Leaders are no longer the ones *"paid for thinking;"* it behooves them to trust and empower their workers. In turn, workers need to trust their leaders to make informed decisions that are in the best interest of the nation. This mutual trust, the first tenet of mission command, is a practical shift from scientific management. Soldiers at the lowest level, oftentimes, are more technically inclined and agile than our senior leaders. Based on this reality, mutual trust is requisite to the continued success of the Cyber force. When Soldiers feel valued and believe that their leaders believe in them, they will be more effective.

FORT GEORGE G. MEADE, Md. -- *A Soldier climbs a rope during the 781st MI Battalion's best warrior competition February 21. (U.S. Army courtesy photo)*

The Cyber Identity: Emergence of Mission Comm

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

An organization's cultural identity naturally matures over time and through foundational shared experiences. The rapid requirement to employ the Cyber Mission Force (CMF) and race to FOC (Full Operational Capability) provided a thin exoskeleton of a functioning basic branch, but at what cost? While not doctrinally aligned with Mission Command, a unified cultural identity within any organization is paramount to successful employment of the defined principles of mutual trust and commander's intent. As critical components to effective and cohesive teams, how do Leaders and Soldiers within the Army's youngest branch effectively embody these values?

The Army as in institution cannot, and does not, implement catastrophic change rapidly. Doctrinal standards and readiness metrics are codified through experience and continued revision as technology and warfare evolves overtime. Prior to Cyber branch's inception in 2014, the most recent basic branches included Special Forces (1987), Psychological Operations (2006), and Logistics (2008). A fundamental difference in their development was mission employment time and experience. Special Forces units were formed in the 1950s, WWII ignited PSYOPs organizations, and the Logistics branch simply unified three pre-existing branches. While the Cyber branch was initially populated utilizing 35Q Soldiers (Cryptologic Cyberspace Intelligence Collector/Analyst), 35A Officers (Military Intelligence), and NSA capabilities, our mission and domain are new and unique territories to the entirety of the DoD.

Despite the initial emergence from MI and NSA ideologies, preferences, prejudices, and risk adversities, how do we develop a new and cohesive Cyber culture? Currently, Cyber "pure" Officers and Soldiers merely skim the ranks of First Lieutenant and Sergeant. This is a stark difference to its sister branches whose Leaders have foundationally served at every echelon; easily exemplifying the Army's utilization of mutual trust through shared experience that fosters the employment of commander's intent. Cyber branch instead creates an inverse reliance of many Leaders on junior personnel for their technical education and team level experience.

Personnel align this dichotomy with a perceived disparity of talent throughout the Cyber force. While this is arguably truthful, we must accept its existence and continue to define the branch's path forward. Displaying confidence and competence in our craft, creating shared experiences, and time will ultimately build mutual trust within the leadership throughout the force. Additionally, with increased mission tempo and authorities, Soldiers and Civilians will

Continued on the next page

FORT GEORGE G. MEADE, Md. *– Bravo Company, 781st Military Intelligence Battalion (Cyber), Soldiers and Civilians executing their Quarterly Attack and Defend training event on November 22, 2019. (U.S. Army courtesy photo)*

mand Fundamentals

Continued from the previous page

propel the branch through operational experience. As personnel continue to serve and migrate throughout the CMF, the mission and risk assumption will eventually evolve to truly meet operational capabilities and requirements. Our task is to enable that history and assist in the definition of the "right" answers.

What ratio of intelligence support to operational capability enables missions? Is there a "technical pure" career trajectory for the branch for both Soldiers and Officers? How much training is too much training? What echelon should approve operational risk? While the list could go on infinitely, the only personnel capable of answering the questions, building the cultural identity, reside within our organizations.

The execution of Mission Command depends heavily upon the foundational pillars of shared understanding, mutual trust, and commander's intent. As the Cyber branch identity continues to develop over time, the vague employment of Mission Command principles will dissipate. It is our Soldiers and Civilians who will pave the Cyber "prop blast" or "spur rides" to create and foster mutual trust and enable execution of commander's intent throughout the force.

FORT GEORGE G. MEADE, Md. *– Staff Sgt. Geoffrey Reck competed in an obstacle course event on February 21 as part of his battalion's 2020 Best Warrior Competition. (U.S. Army courtesy photos)*

CYBER SNAPSHOT: Staff Sgt. Geoffrey Reck

B Company, 781st Military Intelligence Battalion (Cyber)

FORT GEORGE G. MEADE, Md. -- Staff Sgt. Geoffrey Reck hails from Portland, Oregon and is a 35P, cryptologic linguist, assigned to B Company, 781st Military Intelligence Battalion (Cyber). Reck received the Army Achievement Medal for his selection as the Battalion's Best Warrior NCO for 2020 on February 21.

ON WHY HE JOINED THE U.S. ARMY AND BECAME A 17C –

"In response to 9-11 attacks, I wanted to communicate directly with peoples of the Middle East in order to establish better political relationships."

ON WHY HE COMPETED IN THE BATTALION'S BEST WARRIOR COMPETITION –

"To set an example for my Soldiers."

ON WHAT HE LEARNED FROM THIS EXPERIENCE –

"This is my fourth time competing. I gained a vast amount of perseverance and resiliency."

FAVORITE QUOTE –

"The only unfair fight is the one you lose" – Janet Morris

Maintaining the National Trust

By Sgt. Andrew Germek and Capt. Stephen Hart, C Company, 781st Military Intelligence Battalion (Cyber)

In the aftermath of the Watergate scandal and the Vietnam War, Gallup, a well-respected national polling organization, began tracking American's confidence in National institutions. Since 1975, the American people have consistently expressed high confidence in the military (Gallop, November 11, 2019). The military has earned the American public's trust through dominance in the air, land, and sea domains, but trust in its ability to dominate in the cyber domain derives from the military's history and not its actions. Other institutions will challenge the military for American's trust and American adversaries will seek to erode American's trust in the military. As Soldiers and Army Civilians serving in the 780th Military Intelligence Brigade (Cyber), we have inherited that trust from generations before us. Now, it is more vital than ever that we preserve it, so that we may effectively and accountably defend the nation with the hard won confidence of Americans. Cyber warriors face the challenge of preserving trust and confidence when the public cannot verify the military's actions in cyberspace.

The majority of cyberspace operations remain outside of the public scope, but the public is keenly aware of the risk of living in a connected society. Each person with an internet connected device may find themselves under threat from numerous fronts potentially eroding their confidence in any defense. Additionally, most threat actors operate with relative impunity on the internet and their potential for malicious acts increase from the democratization and reproducibility of malicious software. These trends have had far reaching implications to the security of the United States and all nations.

The public's trust for the military in cyber operations must first contend with fierce competition from private sector cyber security. The Department of Defense (DoD) has lost the initial advantage it had on internet technology. It is neither the largest nor the most expert in security when compared with the private sector. The DoD must also compete with the original manufacturer for trust. Partnerships will help transform that disadvantage into an institutional trust building mechanism.

Americans will continue to demand accountability for the expenditure to build the Cyber Mission Force. They will want to see that their tax dollars efficiently spent defending them. However, that remains difficult to prove and verify when cyberattacks on individuals and companies remain rampant. Every success will help improve that trust. Highlighting those successes effectively through public outreach builds trust in otherwise invisible operations.

Trust must originate within the organization. Fundamentally, we obey the laws and policies that guide us, not because we are driven by fear of consequence, but because it is the moral thing to do. We do this, so that our partners and allies both domestically and internationally can trust the 781st Military Intelligence Battalion, the Cyber National Mission Force, and United States Cyber Command to collaboratively bolster the nation's defense. We trust our leaders and commanders to give lawful orders in accordance with national policy as tactical action in cyberspace can have quick strategic impact. These assumptions allow effective teams to build on shared vision and purpose. Further, when leaders at all levels explicitly build mechanisms and controls into their planning that build trust, it ensures that we act purposefully in an otherwise lawless domain.

The challenges of building capability to effectively engage adversaries while remaining accountable can feel painfully burdensome, and it is tempting to envy the Silicon Valley ethos to, "move fast and break things." It is easy to blame lack of progress on some nebulous bureaucracy, but how we as an organization rise to the challenge of building dominance in cyberspace will reverberate for generations to come. The mechanisms we build impose order and drive accountability where little exists in Silicon Valley.

Continued on the next page

CYBER SNAPSHOT: Spc. Ronald Scharch

C Company, 781st Military Intelligence Battalion (Cyber)

Continued from the previous page

Commanders must build trust with subordinates so that soldiers can give an accurate and honest assessment of conditions only seen through sensors. Soldiers must trust that their efforts will have positive effects. Our challenge is to create processes, abide by laws and regulations, and build an organization capable of outlasting any one soldier, so that our organizations can not only withstand public scrutiny and achieve the widespread public support that is necessary for allocating the resources we need to accomplish our mission.

FORT GEORGE G. MEADE, Md. *– Spc. Ronald Scharch completed a 12-mile ruck march (above), and an obstacle course event (below) on February 21 as part of his battalion's 2020 Best Warrior Competition. (U.S. Army courtesy photos)*

FORT GEORGE G. MEADE, Md. -- Spc. Ronald Scharch hails from Cordova, Maryland and is a 17C, cyberspace operations specialist, assigned to C Company, 781st Military Intelligence Battalion (Cyber). Scharch received the Army Achievement Medal for his selection as the Battalion's Best Warrior Soldier for 2020 on February 21.

ON WHY HE JOINED THE U.S. ARMY AND BECAME A 17C –

"I joined the Army for purpose and direction in life. 17C cyber is the future."

ON WHY HE COMPETED IN THE BATTALION'S BEST WARRIOR COMPETITION –

"For the experience."

ON WHAT HE LEARNED FROM THIS EXPERIENCE –

"If you put your mind to it you can achieve anything. I need to focus on regulation knowledge."

ON HIS FUTURE GOALS –

"To make Sergeant and to achieve my bachelor's degree in computer networks and cyber security."

FAVORITE QUOTE –

"You are your own worst enemy"

How the CSD Groks: Commander's Intent and Mutual Trust

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. Because this mission is inherently risky in timeline, scope, and payoff, a paradigm shift is required in both the traditional Army procurement model and how our organizations are built. Fortunately, we have to look no further than the products we develop for inspiration in retooling these constructs to ensure the commander's intent and mutual trust can still be achieved throughout.

To begin the metaphor between software engineering and organizational models, we start at the strategic level since that is where the commander's intent is established. In software engineering, the intent is delivered in a design specification. Such a document lists milestones and defines success along with constraints on the process. Much like a commander's intent, a specification offers a clear and concise expression of the purpose and end state. Together they allow developers to make decisions without further instructions even when events do not turn out as anticipated.

The intent established in the design specification is realized in the form of an Application Programming Interface (API). An interface primarily describes the inputs and outputs of a process. One does not need to know exactly how the process is done, they only need to know what the process expects of them and what they can expect from the process. An API establishes mutual trust in the form of a contract between components and creates a baseline for software assurance and testing. In organizations, these components could be firing crews and staff sections, or mechanisms such as readiness tracking and approving travel for example.

The Unix philosophy further expounds on these ideas to propose minimalistic, composable, design where programs should "do one thing and do it well" rather than complicating existing practices with new features. Organizations often violate this rule by muddying responsibilities or not holding the process accountable when a contract is broken. Instead, they spawn new or duplicate processes that impose additional resource burden and conflict on the system.

These issues can be further mitigated at the tactical level by leveraging component-based design and loose coupling. These ideas are centered on systems composed of independent pieces that are reusable and service-based. They enable autonomous, cohesive teams, and allow organizations to minimize duplication and maximizing redundancy. While these two terms are similar, duplication, as noted above, adds overhead with additional contracts and requirements. Redundancy, on the other hand, reinforces strong, clean, repeatable procedures that can be swapped in and out while maintaining system integrity based on the underlying contracts. All critical to continuity of operations planning and maintaining resiliency to change.

Embracing software engineering principles when designing organizations opens new opportunities for increasing efficiency, shared understanding and mutual trust. While mission command is commonly translated to "subordinates do whatever they need to get the job done", much like spaghetti code, this quickly falls apart in absence of a well-formed commander's intent and without routine validation.

This is how the CSD groks to lead the way in delivering world-class cyber solutions. What is your organization's API?

G R K S

"Devils in Baggy Pants"

By Maj. Brian Lebiednik, executive officer, 782nd Military Intelligence Battalion (Cyber)

"Never tell people how to do things, tell them what you want to do and they will surprise you with their ingenuity" – General Patton

In the Army, we put together groups and ask them to build that mutual trust all the time. Commanders trust that with intent subordinates can plan and execute with little oversight. The fact is that a commander cannot be everywhere at once and through time build trust in their Soldiers and Civilians to take their intent and execute violently. Through a common core of PME (professional military education) and collective training, we build superior teams that share a common vision and work with mutual trust. In my mind, nothing exemplifies this better than the concept of Little Groups of Paratroopers (LGOPS).

Back in WWII, commanders did not have Blue Force Tracker or UASs (unmanned aerial systems) to watch the movements of their formations. They had to trust their Soldiers would execute the intent without question. If you have ever done an airborne operation, you understand that airborne commanders need to trust more than most. High winds or missed drop zones can cause havoc even on training missions. During one of my first airfield seizures, my company barely massed enough combat power to have a support by fire element and assault element.

During the invasion of Italy, Operation Husky occurred during a night that boasted 35 to 45 mile per hour winds. Gliders crashed, planes flew off course. Less than half of the Soldiers made it to their rally points. Despite all of this, a German Soldier remarked, "American parachutists … devils in baggy pants … are less than 100 meters from my outpost line… Seems like the black hearted devils are everywhere …". The 505th Parachute Infantry Regiment LGOPS continue the mission with the commander's intent and 504th PIR earned their nickname "Devils in Baggy Pants".

Looking back at the D-Day invasion, LGOPS landed scattered throughout the French countryside. Each operated on a couple shared principles that ensured the trust of the groups. They shared a common vision, knew the mission intent, and took initiative. This turned the airborne operation from a potential disaster to an incredible success. They had even trained to build mutual trust between companies well before the invasion. The 18th Airborne Corps Commander, Maj. Gen. Matthew Ridgeway, forced them to do intermural sports with teams mixed with Soldiers from different companies.

The fact that Soldiers from different units could combine to harass the Italian and German Soldiers without ever working together is a testament to the trust that they built. They massed LGOPs where available and executed the commander's intent to the best of their ability. The concept of LGOPs still rings true in everything that we do today. We build the mutual trust and empower our subordinates to execute violently.

American Paratroopers of the 504th Parachute Infantry Regiment

Building Better Teams through Mutual Trust: Lessons Learned from 9/11

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

The haunting attacks of 9/11 took most of the world by surprise, but not everyone watched the events of that day unfold in total disbelief. There were several elements within the intelligence community (IC) which understood the growing threat posed by radical Islamist terrorism and warned senior leaders about a desire to attack the United States. However, a lack of mutual trust amongst the different agencies caused a failure to share and corroborate the relevant information needed to help thwart the attack. The U.S. intelligence apparatus has many distinct nodes with slightly different purposes, but ultimately their goal is the same: to provide information that will protect the United States and maintain its status as a global leader. So if all these entities are on the same team, why is it so difficult to create mutual trust? It may be petty rivalries or a competition for limited funds, but whatever the reason, most people can agree that the lack of cooperation and trust did lead to disaster on the morning of September 11, 2001.

The threat of a "Cyber Pearl Harbor" is a well-known concept which helped elevate the importance of, and need for, a U.S. Cyber Command. This ominous danger brings awareness to potential vulnerabilities in our national infrastructure and led to an emphasis on creating and maintaining a strong defense. To this end, the majority of Army Cyber Command's focus is on defense tasks. Defense is undoubtedly important; however, a threat like that of 9/11 could be neutralized through the coupling of an aggressive offense and mutual trust of the organizations involved. Like the actual events of 9/11, a "Cyber 9/11" would likely not be crippling to our national infrastructures, but such an event would certainly deal a blow to our national ego. Had more trust existed within the IC in 2001, there is a good chance the terrorist events could have been stopped. In the same vein, we can lean forward and prevent such a cyberattack by restoring trust within the bureaucracy and allowing us greater latitude to execute offensive actions.

Trust is mercurial and, most often, only earned through time and experience. U.S. Cyber Command was created in 2009 and over a decade later, our Mission Commanders and Team Leads still have not earned the full trust of senior decision makers. Or at least, that is how it currently appears. Commander's intent is overly specific for cyber missions, leaving almost no room for our mid-level leaders to exercise the tenets of mission command. An Infantry Platoon Leader is trusted to make decisions on the spot to keep dozens of Soldiers alive on dangerous missions. Meanwhile, some of the most technically savvy men and women in the U.S. Army today are not trusted to operate on keyboard – precisely the activity they were recruited to perform.

Why this trust is lacking is not exactly clear. Perhaps planners automatically associate the term "cyber" with strategic connotations and assume it requires the associated high-level authorities. Perhaps the field is too new and those responsible for prosecuting war in this new domain are afraid of consequences as yet unseen or unknown. Perhaps money is a factor and shot callers are afraid funds will be diminished as a result of one mistake. It may even be because the Cyber branch was built out of the Military Intelligence Corps, which has a culture of oversight and compliance. What is clear: mutual trust is a key tenet of mission command and as a military organization, we cannot operate effectively if we continue to ignore the necessity of its employment.

Similar to personal relationships that lack trust, the most important factor in building trust is effective communication. From a junior to mid-level leader perspective, that means laying out missions in terms that non-technical leaders can understand. The mid-level leader should think at least two levels above and try to understand the risks seniors are worried

Continued

Mutual Trust: Its Presence Amidst Gestalt Theory & the Coalescence of a Team

By Capt. Ian Howard, C Company, 782nd Military Intelligence Battalion (Cyber)

Mutual trust permeates the continual development of a functioning team. A team bound by mistrust and misunderstood intentions of one another's actions is destined to fail long before the arrival of a mission's end state. The concept of mutual trust appears on a multitude of occasions throughout the history of famous war scenario studies and infamous leaders of example, but is rarely mentioned regarding its presence throughout particular team dynamics.

Gestalt Theory – the emphasis that the whole of a group in its entirety is greater than the sum of its individual parts. Mutual trust is undoubtedly an important undercurrent to this lesser mentioned concept. Amidst the lifecycle of a thriving team, mutual trust serves as the bonding agent that compounds a team's effectiveness – not in just social connections, but the collective trust that every contributing teammate has in one another. A team without mutual trust is bound to suffer diminishing returns, whether it is mission accomplishment or the quality of a product demanded of a struggling Analysis and Production cell.

Army service members are no strangers to joining a different team – whether it's a new company or an entirely new post. We experience a shift of social dynamics when moving into a new ecosystem. In many occasions, amidst the beginning of a new team with a majority of members whose residency is rather young, Soldiers must build from the ground up and progress through the "form, storm, norm, perform" stages of team coalescence. What's peculiar is that mutual trust serves as a major turning point in the cycle of the team's development. It is at the end of the "storm" phase, and entering the "norm" phase of a team's bonding that mutual trust catalyzes the team's progress towards autonomous functionality, as well as the ability to cooperate seamlessly without the worry of misunderstood intent of action.

Though brief in depth, it's important to realize that mutual trust is a pervasive team element that progressively affects multiple realms of a unit's dynamic. A team's effectiveness is more than just tethered to the sometimes unforeseen realm of mutual trust, but bound to it on a constant basis.

FORT GORDON, Ga. *– Sgt. James Ware represented C Company during the 782nd Military Intelligence Battalion's Best Warrior Competition. (U.S. Army photo)*

Building better teams (cont.)

about, and they must have a plan to mitigate such risks. They need to clearly articulate what will be lost if something goes wrong. Ultimately, if American lives are not being lost, what is the real risk in certain cyber missions? Creating mutual trust takes time, but the only way for someone to truly maintain such trust is to have it given to them, and then proving they are worthy of it by protecting it and giving trust in return.

In the pre-9/11 era, we forgot we were on the same team. We must remember that we all have the same goals in the cyber domain: to protect the United States. At the end of the day, a good offense is the best defense. We must be willing to give and return trust. Without mutual trust, we cannot have a shared understanding. Without a shared understanding, our ability to operate along a common operating picture is diminished irreparably. Are we really going to wait until something terrible happens before we start trusting our subordinates?

Generation Cyber: Developing Tomorrow's Cyber Mission Force

By Capt. Jordan W. Salyer, 102 CST lead, A Company, 782nd Military Intelligence Battalion (Cyber)

The Cyber Mission Force has grown significantly over the last ten years, from small separate subsets of personnel mostly working out-of-site and out-of-mind of U.S. leaders, to the unification of these subsets as United States Cyber Command and daily coverage of cyber incidents from every major news outlet around the world. It is no secret the world is increasingly becoming "connected" and new technology is being developed every day; therefore, the spotlight is on cyberspace and the actions taken within it. In such a chaotically evolving new domain, the principles of Mission Command are more critical than ever. Creating shared understanding, ensuring clarity of the Commander's Intent and building mutual trust among the Cyber Mission Force (CMF) – along with the other principles of Mission Command – are paramount to the growth and continued success of the CMF.

We have a new generation of Cyber warriors that have lived their entire lives in a digital world, and as such, the cyberspace domain is second nature to them. The Services spend thousands of dollars per person on lengthy training pipelines to ensure they are competent within their roles. The complexity and sheer size of this domain make it imperative to rely on and trust our subject matter experts to provide senior leaders with effective operational counsel. The CMF must leverage this knowledge and understanding to give the Combat Mission Teams (CMTs) and other mission partners more freedom of movement to accomplish these operations.

One aspect that can help freedom of movement is increasing our tactics, tools, and techniques for use in cyber operations. This is an ever-growing requirement among the CMF to ensure our initiatives are carried out effectively. With that said, this does not mean we need to spend millions of dollars to create new and overly complex systems for operations. The CMF can use or repurpose openly available tools that blend in with all the gray traffic already consuming the internet. If the Commander's Intent is clear and concise with the purpose, key tasks, and desired end state, the mission force should be allowed to use whichever tactics, tools, and techniques (TTTs) fit best to effectively complete those actions. The Offensive side of the CMF is too risk-averse when it comes to cyber operations, often erroneously focusing specifically on the custom tools. Not only does this stifle creativity among the populace, but it also breeds a perfunctory environment. Reusing and repurposing publicly available tools as previously stated, would allow the forces to expand their capabilities and foster a dynamic force. This is where mutual trust between the leaders of the CMF, and the Operators' technical expertise, is key to providing an environment of creativity and encouragement to allow the freedom of thought for new TTTs.

The importance of having a clear understanding of the Commander's Intent and mutual trust at all levels cannot be overstated. Using these and the other tenants of Mission Command as previously discussed, we can expand our capabilities and develop tomorrow's CMF as a more agile and effective force.

CYBER SNAPSHOT: Spc. Steffan Hinkle

A Company, 782nd Military Intelligence Battalion (Cyber)

FORT GORDON, Ga. -- Spc. Steffan Hinkle hails from Osceola, Florida, and is a 17C, cyberspace operations specialist assigned to A Company, 782nd Military Intelligence Battalion (Cyber). Hinkle received the Army Achievement Medal for his selection as the Battalion's Best Warrior Soldier for 2020 on January 24.

ON WHY HE JOINED THE U.S. ARMY AND BECAME A 17C –

"I joined the Army to serve my country, hoping to make a difference, while setting a path for my Family's future. 17C was a clear choice as I had always worked a lot with computers and developed a passion for it. Over time everything will continue moving online and the cyber domain will become more and more crucial."

ON WHY HE COMPETED IN THE BATTALIONS BEST WARRIOR COMPETITION –

"Being new to the unit and my first duty station, it gave me the opportunity to test myself and see what I could accomplish."

ON WHAT HE LEARNED FROM THIS EXPERIENCE –

"I learned that focusing on one event at a time can make all the difference, instead of worrying about the whole competition as a whole."

ON HIS FUTURE GOALS –

"Short terms goals are to reenroll in school and complete a bachelor's degree in computer science, as well as be promoted to sergeant and become fully job qualified with my current work role. Long term goals are to move from a bachelor's degree and complete a masters. As well as continue climbing the ranks and learning various job roles so that I can be more beneficial to my team."

FORT GORDON, Ga. *– Spc. Steffan Hinkle hails from Osceola, Florida, and is a 17C, cyberspace operations specialist assigned to A Company, 782nd Military Intelligence Battalion (Cyber), headquartered at Fort Gordon, Georgia. Hinkle drags a 90-pound sled on January 22 as part of the Sprint-Drag-Carry event (left), and finished second overall in the 12-mile ruck event on January 23 (above). (U.S. Army photos)*

780TH MILITARY INTELLIGENCE BRIGADE

SOLDIER OF THE YEAR

SPC STEFFAN HINKLE

780TH MILITARY INTELLIGENCE BRIGADE

NCO OF THE YEAR

SSG GEOFFREY RECK

Mutual Trust - Critical Ingredient: Cyber Warriors,

By Capt. K. Lee Shelton, commander, B Company, and Capt. Ian J. Reynoso, commander, D Co., 782nd MI Battalion (Cyber)

Custer's Last Stand by Edgar Samuel Paxson (1852–1919) - Whitney Gallery of Western Art

As cyber teams build and train to meet emerging threats in the future, as well as answer an ever-increasing demand for support to combat operations, we must get better at not only applying but also understanding mutual trust. Trust is the solid floor on which the success or failure of an organization's leader-Soldier relationships is built upon. Given that majority of our day-to-day work involves heavily relying on each other to accomplish our mission and objectives, mutual trust is single handedly the most important characteristic of a successful organization. As individuals, we are often entrusted with getting a task completed, showing up to important meetings, being an expert at our job, and completing a mission successfully. The problem faced most often in organizations, including ours, is that trust is a commodity. Trust is very difficult to build and yet is extremely fragile.

Perhaps the most infamous figure in American military history representing a failure of trust was General George Armstrong Custer. We can learn from Custer that despite resounding victories at a young age, lack of mutual trust can lead to disaster. As the authors, we both have explored and researched Custer's successes and failures. We will make an attempt to reflect on how mutual trust was a key factor in his failure while maintaining relevance to our growing and complex cyberspace battlefield today.

Considered one of the worst American defeats in western military history, the Battle of the Little Bighorn clearly displayed the outcome when the principles of mission command, specifically mutual trust and commander's intent, are not clearly understood or implemented by leaders during decision making and mission execution. The effects of poor leadership displayed by the officers of the 7th Cavalry have been criticized even over a century later. To better understand the value and importance of trust and intent, we will look at the actions taken by General George Armstrong Custer, commander of the 7th Cavalry Regiment.

General Custer was without a doubt a daring, flamboyant leader. During his time in the Civil War, he made his name by leading his men in the face of overwhelming odds and achieving mission success. His men naturally gravitated towards his bold leadership style. Custer's superiors praised him for his natural ability to size up enemy forces, predict their actions, and make split-second decisions that almost always ended in resounding victories. After the Civil War, Custer was assigned to commands in both the southern and western United States. During this time, he became bored with his new assignments and therefore he also became complacent.

Cohesive Teams Required

This is not so far away from what we experience in the cyber strata. It's no surprise that some of the cyber assignment's Soldiers find themselves in, at times, boast of boredom and apathy. This then breeds an environment of complacency and purposelessness. In the complex and challenging environment where we operate, making tough on the spot decisions is no longer one of the biggest challenges. Instead, the challenge lies in producing an environment where individuals feel like they have ownership and empowerment in the organization they work for. Soldiers must be able to give all of their effort to every assignment no matter how insignificant it may seem. Leaders must demonstrate how every position is needed and be able to explain why every position needs a good Soldier. As General Patton once said, "I am a Soldier, I fight where I am told, and I win where I fight." Soldiers find this spirit by being entrusted with responsibility. We will examine how Custer failed to do this and ultimately what it did to his mission and men.

It is clear through historical documentation that Custer began to exhibit an attitude of disdain and disrespect for those Soldiers that did not share his love of the Army or of battlefield combat. He treated his Soldiers harshly and handed out cruel and unusual punishments, yet he failed to follow the regulations that he himself was enforcing. Only those who were close friends or family were treated with any sense of civility. We should tread very carefully with this in cyber. The greatest folly of this behavior was the fact that Custer actually believed that he was justified in his actions. He believed he was above the law and that the regulations were what he said they were, and applied to whomever he said they applied. These actions and his example contributed to a toxic environment and fueled a hatred and distrust of him among his subordinates, to include many of his officers. Ten years later when he was leading the 7th US Cavalry up the Rosebud River to their defeat at the Little Bighorn River, these feelings of distrust and lack of confidence in Custer still lingered among his men.

The cyber branch is young, and growing pains abound. The time is now to begin building trust amongst all Soldiers and civilians in the cyber field, instead of burning bridges. We are a small group, and our actions will be remembered by those we serve with. What will your Soldiers and battle buddies remember about you ten years from now?

Prior to the Battle of Little Bighorn, General Custer seemed to do quite well at creating a shared understanding of the enemy problem set which his units were facing. At the Battle of the Washita River, he ensured his mission success by correctly estimating the enemy's strength, sharing it with his subordinates, and giving precise direction to his commanders. Their orders were to surround the enemy on four sides, creating a multi-pronged attack. His officers executed their tactical tasks and surrounded the enemy Indian village. In an almost simultaneous, fluid action, they all attacked and defeated the enemy within a short time. One of General Custer's lieutenants, Godfrey, had scouted ahead during the battle after completing his task of securing the enemy's pony herd. He found several more Indian villages across a ridge from Custer's 7th Cavalry, and rode back to inform his commander. Several other scouts were reporting additional enemy Indian units in the area as well. Custer then made the correct decision to leave the area lest his command be overwhelmed by a superior force.

What a great example of what we SHOULD do as leaders and subordinates. Custer's subordinates knew he respected their opinions, and knew that he would listen to them. He did listen to them and made the right decision, despite his normal attitude of arrogance and narcissism. Do we do this in cyber? Are the senior leaders really listening subordinates? We are not picking on any one group here, but want to drive home the idea that leaders at all levels need to listen to Soldiers in the trenches, else they risk making an incorrect, un-informed decision. By the same token, junior Soldiers need to understand and learn to recognize wisdom in senior leaders. They

Continued on page 47

Multi-Domain Operations in the 1930s vs Today

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

U.S. Marines participated in a series of limited conflicts in Mexico, Central America, and the Caribbean from 1898 to 1934, now collectively known as the Banana Wars. The post-WWI engagements in Nicaragua are especially important because they were a time of innovation for the U.S. military – where ideas from the Western Front could be tested in a combat environment to create concepts and tactics for future large wars. It was during this time that President Coolidge deployed 2,000 Marines to Nicaragua to intervene in a civil war, resulting in the first documented dive-bomb raid in history.

On July 16, 1927 in Ocotal, Nicaragua, 600 rebel forces led by General Augusto Sandino attacked the combined force of 89 U.S. Marines and Nicaraguan guardsmen. Two marine aircraft conducting a routine flight noticed the battle and returned four hours later with five DH-4 biplanes equipped with two machine guns (one on the nose and one on the tail) and four 25-pound bombs. The marine aviators dived from 1,500 feet, strafing enemy positions and releasing bombs only 300 feet above ground, killing approximately 60 enemy fighters and saving the defenders from certain defeat.

Thus started a series of battles where the Marines paired air power in support of ground forces. In 1927, synchronizing operations between the two warfighting domains required a great deal of coordination, planning, and rehearsals. Most importantly, it relied on mutual trust and complete understanding of the commander's intent.

The ground forces commander had to trust that air support would be present at the agreed-upon time during the battle. Without this mutual trust, ground troops could not have the confidence to maneuver against a fortified position. The Marine infantry could not even verify that the air support was en route! Today, this coordination happens at the speed of light, but in 1927 it relied completely on mutual trust that the aircraft would be on target at the specified time.

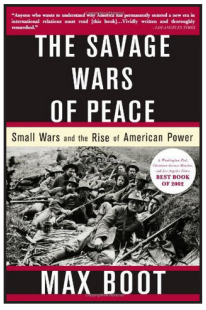
Commander's intent is interwoven with mutual trust, to ensure that both forces understand what is expected of them – to understand their boundaries during the operation and drive all units (on the ground and in the air) toward a common goal.

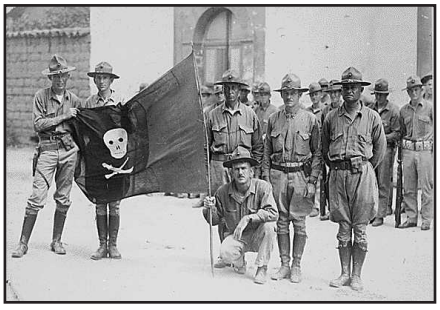
This is no different to Joint operations conducted today and it is even more relevant as it relates to cyberspace operations in support of land, sea, and air operations. In a hypothetical Joint cyber/naval operation, cyber teams may not be co-located with U.S. warships conducting freedom of navigation operations in the South China Sea. The cyber team must understand the U.S. Pacific Fleet commander's intent for that operation in order to create the appropriate supporting effects.

Even more difficult, the U.S. warships will need to place their trust in that cyber team, thousands of miles away, operating at a classification level that may restrict communication about what the cyber team will do. This mutual trust will not come over night – it will take years of practice, at combat speed, to develop these relationships.

Fourteen years after the battle of Ocotal, Nicaragua, the United States entered World War II, getting a chance to test the dive-bombing techniques developed by that small group of Marines. The U.S. Army activated the 780th Military Intelligence Brigade (Cyber) nine years ago. Are we in the midst of an inter-war, innovation period now? Are we properly testing concepts that will be used in a large war five years from now? Time will tell...

If you are interested further reading about the small wars that U.S. forces conducted over the past 220 years, I highly recommend "The Savage Wars of Peace: Small Wars and the Rise of American Power" by Max Boot.





CYBER SNAPSHOT: Sgt. Christopher Owens

E Company, 782nd Military Intelligence Battalion (Cyber)

FORT GORDON, Ga. -- Sgt. Christopher Owens (center) hails from Allentown, Pennsylvania, and is a 17C, cyberspace operations Noncommissioned Officer (NCO) assigned to E Company, 782nd Military Intelligence Battalion (Cyber), headquartered at Fort George G. Meade, Maryland. Owens received the Army Achievement Medal for his selection as the Battalion's Best Warrior NCO for 2020 on January 24.

ON WHY HE JOINED THE U.S. ARMY AND BECAME A 17C –

"I joined the Army to serve my country, hoping to make a difference, while setting a path for my Family's future. 17C was a clear choice as I had always worked a lot with computers and developed a passion for it. Over time everything will continue moving online and the cyber domain will become more and more crucial."

ON WHY HE COMPETED IN THE BATTALION'S BEST WARRIOR COMPETITION –

"Being new to the unit and my first duty station, it gave me the opportunity to test myself and see what I could accomplish."

ON WHAT HE LEARNED FROM THIS EXPERIENCE –

"I learned that focusing on one event at a time can make all the difference, instead of worrying about the whole competition as a whole."

ON HIS FUTURE GOALS –

"Short terms goals are to reenroll in school and complete a bachelor's degree in computer science, as well as be promoted to sergeant and become fully job qualified with my current work role. Long term goals are to move from a bachelor's degree and complete a masters. As well as continue climbing the ranks and learning various job roles so that I can be more beneficial to my team."

FORT GORDON, Ga. *– Sgt. Christopher Owens hails from Allentown, Pennsylvania, and is a 17C, Cyberspace Operations Noncommissioned Officer assigned to E Company, 782nd Military Intelligence Battalion (Cyber). Owens qualified with his M4A1 Rifle on January 22 as part of his battalion's 2020 Best Warrior Competition. (U.S. Army photos)*

Mutual Trust and Commander's Intent

By Lt. Col. Jason P. Hogan, commander, Detachment-Hawaii, 782nd Military Intelligence Battalion (Cyber)

"This world of ours… must avoid becoming a community of dreadful fear and hate, and be, instead, a proud confederation of mutual trust and respect."
Dwight D. Eisenhower

It is too easy in today's workforce to sow seeds of discontent and mistrust for fear of change, fear of the unknown. Turning the known unknowns into the known knowns is the job of the Command teams. There exists in this Brigade, a dynamic blend of Soldiers and Civilians, many of whom served as uniformed members of our Armed Forces, multiple requirements from varying services, and a unique challenge to balance egos of an intellectually and emotionally gifted workforce. Command teams must demonstrate trust, treating its employees with dignity and respect, and convey a vision based on shared ownership. In this world of give and take, it is the members of the Brigade to responsibly champion for one another in all things, and trust that their leaders are providing advice, information, and truths to the Commander so he or she can make the best decision for the good of the mission and the organization. We must each only take actions that help foster an environment of trust and respect.

Why Commander's Intent? What does it do? In the simplest of terms, it provides a vision, an end-state, and a conceptual goal for an organization. When the Commander is absent or busy, this simple section of an order (or likely PowerPoint!), keeps the team working in a unified direction and enables staff to make decisions in-line with the commander's vision.

A source of frustration over the last eight years in this Brigade, staff many times make a decision they do not have the authority to make. Staffs make recommendations; commanders make decisions. In the commander's absence, this intent allows staff to plan and execute a task and give guidance to subordinate organizations. When staff officers and primaries do not understand the commander's intent, they often give out misinformed, although well intentioned, inaccurate guidance as the commander's decision. I have seen this at team levels and at organizational leadership levels. If you as a Soldier or Civilian do not understand your Commander's Intent, plan on executing it violently, or disagree with it, you have work to do on yourself.

What we are really discussing here is the combination of the science of leadership with the art of leadership. A question once posed to me during a board was:

> *"What is more important? That you are right or that people listen to you."*

There is no defined, good answer to this question. However, what is the point of being right if no one listens to you and what happens if people listen to you but you are wrong? The latter is a dangerous position that does a disservice to your Soldiers and Civilians.

Finally, trust is a two way street and a balancing act. "Mission First, People Always." As a Commander, I trust you implicitly and unconditionally to accomplish the mission, whatever that mission is, and protect and improve the unit and each other. Commanders want and need you to give them the same unconditional trust; perspective imbues a command team with a macro view, receiving inputs from its members, higher headquarters, adjacent commands, and other organizations, and your command teams need you to trust that they are working for you not against, that they have the mission and organization's best interests in mind. Your input is valued yet weighed against the orders

Continued on page 46

Mutual trust and commander's intent in a Joint, interagency environment

By Capt. Kyle Yoder, 401 CST Team Lead, Detachment-Texas, 782nd Military Intelligence Battalion (Cyber)

Mutual trust is key to the successful operation of any cohesive organization, military or otherwise. Commander's intent allows units to function autonomously while remaining a part of a larger whole. The continued integration of multiple service teams under each JFHQ-C (Joint Force Headquarters – Cyber) builds a dynamic environment that requires effective use of the tenants of mission command, which allows different teams to achieve the same objective. The unique perspective teams bring across normal service lines opens new opportunities for all services to grow. These teams show their trust as they not only work together to accomplish the mission but rely on members from across all services to train new team members in all work roles. The JFHQ-C commanders show trust and give clear intent, allowing the best team to work the mission without undo oversight. The coordination among the teams and the headquarters continues to build a better Cyber Mission Force.

As each service works to grow their own cyber forces, different and sometimes divergent training plans have arisen. The different services have created their own training to bring their personnel up to the standard needed to complete the missions assigned to them by the JFHQ-C. However, while knowing services have different training pipelines to get team members ready for mission, the teams all work together to fill adjunct faculty positions and training each other for specific work roles. As a cohesive Cyber Mission Force, the unity and trust built among the teams working in a joint environment will build the fighting force needed for the future. Demonstrating this, over the last year alone, one Army team single-handedly has trained over 200 Soldiers, Sailors, Airmen, Marines, and DOD Civilians as a part of the adjunct faculty program.

As the separate services work together, their differences influence how a team will approach and subsequently accomplish a mission. Because of these different approaches, commander's intent plays a pivotal role in success. The JFHQ-C (Air Force) Commander's guidance to the teams that make up his command, no matter the branch of service, is a key example of the execution of effective mission command. Although an Army team may take a completely unexpected tactical approach compared to an Air Force team, if the commander provides clear and complete commander's intent, both teams will be able to accomplish his desired end state.

Building on commander's intent, a prime example of mutual trust in execution is the JFHQ-C (AF) Commander assigning Army teams a top priority within his command. The JFHQ-C (AF) Commander chose the teams he felt best for the mission, and in this case, they are majority Army teams. This choice demonstrates the trust the commander has in Army teams; trust to effectively complete any mission he assigns them regardless of service. Then, when this priority required a Task Force, he turned to an Army team for his Task Force Commander, again putting those with the right expertise in charge of the mission. Building a command environment where trust across service lines can be shared up and down the chain of command allows the nation to be a dominate force in cyber space.

Looking to a third sister service the Marines, General Jim Mattis captured his stance on trust and commanders intent in his book, "Call Sign Chaos: Learning to Lead":

> *"You don't control your subordinate commanders' every move; you clearly state your intent and unleash their initiative. Then, when the inevitable obstacles or challenges arise, with good feedback loops and relevant data displays, you hear about it and move to deal with the obstacle."*

Continued on page 46

Cyber Trafalgar

By Maj. Luis A. Etienne Jr., executive officer, 915th Cyber Warfare Battalion

The Battle of Trafalgar, as seen from the starboard mizzen shrouds of the Victory. J. M. W. Turner (oil on canvas, 1806–1808)

Abstract

A few years ago, I read a fascinating book written by Gen. (retired) Stanley McChrystal, Tantum Collins, and Chris Fussell named "Team of Teams: New Rules of Engagement for a Complex World." This book presents different historical and contemporary vignettes, as well as the experiences of Gen. McChrystal throughout his illustrious career, as case studies of the complexities government and private sector organizations face in today's contemporary operating environment. One of the vignettes discussed Vice Admiral Sir Horatio Nelson and the Battle of Trafalgar. While reading about Lord Nelson and his superior tactical performance in battle, I couldn't help noticing the applicability of the lessons learned in this vignette to achieving success in Cyber Operations. The following is a brief description of the events that occurred during the Battle of Trafalgar and my thoughts on the application of the lessons learned to conducting cyber operations at the tactical levels.

Historical Recap of the Battle of Trafalgar

In 1805 Napoleon Bonaparte was the newly crowned emperor of France, and was sweeping through Europe conquering everything in his path. Although he experienced a great deal of successes throughout the Napoleonic Wars, the proverbial thorn at his side was Great Britain, her resources, and her superior Navy. As Napoleon faced the many coalition of nations during the war, England was always there supporting those coalitions with her extensive resources and massive trade network. She provided finance, supplies, and the support of the Her Royal Majesty's Navy to every coalition trying to topple Napoleon and his forces. Napoleon knew that a major factor in the continuance of his conquest and expansion would be the successful invasion of Great Britain, and this was no easy task. The primary obstacle preventing Napoleon from landing forces on British soil was the fact that his Navy was far inferior to that of Great Britain's. Every previous attempt made to get past the massive blockades of the British Navy was thwarted.

In September, 1805, the French and Spanish Armadas, under command of Admiral Pierre de Villenueve, were blockading the Port of Cadiz. Napoleon, seeing an opportunity to gain a foothold in the Mediterranean, instructed Villenueve to move east towards the Strait of Gibraltar to wreak havoc along the way. Villenueve made an effort to reach the Strait of Gibraltar while his forces were pursued by the much faster and more agile British fleet commanded by Vice Admiral Sir Horatio Nelson. Admiral Villenueve soon realized he was not going to be able to outrun the British forces in pursuit, and ordered his fleet to return to the Port of Cadiz.

Unfortunately for him and his men, this order came too late. As Villenueve and his fleet attempted to return to the port of Cadiz, Lord Nelson and his fleet were waiting for them at the Cape of Trafalgar.

Lord Nelson knew that victory against Villenueve meant a decisive blow to the naval power of Napoleon, and a major blow to the Napoleon's efforts. Conversely, defeat of Lord Nelson's fleet would leave the defenses of the British Island vulnerable to Napoleon landing ground forces for an invasion. Outnumbered 27 British vessels to Villenueve's 33, Lord Nelson and his Sailors had a daunting task ahead of them. However, the British had a subtle, yet significant, advantage over Villenueve and his armada: the tactical genius of Lord Nelson. Known for his uncanny ability to maneuver his vessels to victory, Lord Nelson crafted a plan to divide and conquer Villenueve's force. Traditionally, opposing naval forces engaging in battle at sea would line up parallel to each other in a bow to stern formation, and the forces would fire upon each other until one side was destroyed or surrendered. Lord Nelson understood that Villenueve was expecting this and used this expectation to his tactical advantage. Instead of lining up parallel to Villenueve's forces, he would have his forces form two parallel lines and conduct a perpendicular attack on Villenueve's fleet, separating them into three decentralized entities. The end-state of separating and confusing Villenueve's forces did not come without risk. His forces were going to have to maneuver head-on to the enemy formation without being able to fire back until the French and Spanish fleet was split. However Lord Nelson knew that this tactic would cause confusion, and once Villenueve's fleet was split, it would provide his forces a decisive advantage. On September 21, 1805, Lord Nelson and his fleet executed the plan marvelously. Although Lord Nelson was mortally wounded during the battle, his men performed admirably and his plan proved a success. After several hours of battle, Villenueve's fleet was destroyed. Dubbed the Battle of Trafalgar, the Franco-Spanish naval defeat saw the permanent crippling of the Spanish navy. The French were hit hard, but over time were able to recover and rebuild most of their fleet. Nevertheless, the victory for Lord Nelson and his fleet further solidified the naval dominance of Great Britain throughout the remainder of the Napoleonic Wars.

Lessons Learned for Battle in the Newest Domain

As I read this vignette on the Battle of Trafalgar, I was astounded by how much of the lessons learned were applicable to several aspects of Cyber Operations at the tactical level. The leadership, creativity, and preparation of Lord Nelson and his fleet are a blueprint of the qualities necessary in leaders and Soldiers operating in the Cyberspace domain.

Lord Nelson's tactical success during the Battle of Trafalgar was less about the specific tactic he used and more about his ability to think outside the box. There is nothing overly complex about attacking a linear formation from its side, splitting the formation into three decentralized parts, and attacking three separate disorganized and decentralized formations. Lord Nelson's ingenuity was not in the tactic as much as his refusal to line up his formation parallel to that of his opponent for battle. Lord Nelson knew the tactics of his enemy, understood the weakness in those tactics, and was willing to exploit those weaknesses through divergent thinking. Similar to the maritime variables Lord Nelson had to consider (weather, visibility, and surface behaviors), the Cyber Operator today faces countless variables and factors that impact the Cyber environment. Creativity is a necessity to operate in Cyberspace. The inability to recognize the need to deviate from a plan when operating in such a complex environment, leaves forces unprepared to deal with the exponential amount of environmental changes that could occur.

Lord Nelson's success against the larger Franco-Spanish fleet was not only due to his ability to tactically think outside the box, but also his unwavering faith in the competence and ability of his subordinate leaders. This confidence was gained through the meticulous planning and preparation he did with his subordinate leaders. The level of confidence he had in his men could not be more evident than in the British Fleet's execution of Lord Nelson's attack plan during the Battle of Trafalgar. As mentioned earlier, traditional battles at sea had the opposing forces line up parallel to one another and bombard each other with musket and cannon fire until either side suffered enough losses of men or ships to declare a victor. Element commanders would position their ships in the center of the formation

Continued on page 49

Developing a Culture of Military Discipline

By Capt. Allyson I. Hauptman, company commander, Headquarters & Headquarters Company, 915 Cyber Warfare Bn.

New frontiers are often envisioned as lawless, unregulated terrains in which anything goes. Just dive into your favorite Westerns or space odysseys, where the antagonist is usually the law itself. These movies normally end with the heroes reclaiming the frontier for the "good guys," never tackling the harder question of "what next?" Establishing something is easy; whereas, building it into a lasting, strong, cohesive organization is difficult. In establishing the Cyber Warfare Battalion (CWB), the Army created one of its most MOS-eclectic organizations and filled it with excited, hard chargers who sought an opportunity to make a lasting impact. An organizations full of motivated individuals is both a commander's dream and nightmare. On one hand, it is impossible to generate the same level of hard work and investment from unmotivated Soldiers. On the other hand, if the unit lacks a strong culture of military discipline, these same Soldiers are impossible to organize and focus towards the commander's intent. This is why it is vital that the 915th CWB develops a culture that simultaneously rewards individual initiative while emphasizing the importance of military discipline and commander's intent.

One of the best ways to focus a group of individuals towards a common goal is to foster healthy competition. The CWB's Commander's Cup initiative is designed to encourage individual creativity and effort while enforcing the importance of military discipline and Soldier tasks. The pilot iteration of this quarterly intra-battalion competition consisted of a capture-the-flag cyber exercise and a field training exercise, the ladder of which included a road march, marksmanship, casualty care, and radio communications. Soldiers competed in buddy teams of their choosing, and the winning team consisted of both a company grade officer and a non-commissioned officer. The Commander's Cup emphasizes to all of the Soldiers in the battalion that their leadership values intellect, creativity, fitness, discipline, and teamwork, and that all of those attributes are key to our unit's success.

Healthy competition thrives nowhere better than during Physical Training (PT). Daily PT is a cornerstone of how we are shaping our unit culture, at both the company and battalion levels. PT provides all Soldiers the opportunity to develop and lead workouts and encourages all Soldiers in the unit to exercise military discipline in following directions from the PT leader, regardless of his or her rank. PT Leaders showcase their ability to compose a workout that fulfills the commander's intent. That being said, our unit PT calendar also allots time for Soldiers to perform individual or section PT that is tailored to their personal fitness goals. The reason for this is that no one, not even the most disciplined Soldier, wants to be micromanaged all the time. They need some breathing room to pursue personal goals, including fitness goals. Finding the right balance between individual and unit PT is a vital component of maintaining a force that is both motivated and disciplined.

But what is that balance? When CWB officially activated in May of 2019 it was operating piece-meal out of multiple buildings. Soldiers might go all day without seeing a single member of their leadership. It was an unsustainable situation, because with every additional Soldier the unit obtained, the more chaotic and harder to exercise command and control it became. CWB leadership faced a dilemma- should they immediately move the battalion into its new temporary spaces before they were properly outfitted or continue to spread itself out over a multitude of buildings across post. They opted for the former, because the technical challenges of outfitting a building while occupying it were outweighed by the risk of losing the chance to define the CWB's culture and develop it as a disciplined, effective fighting force. Those technical challenges were not insignificant, but the highly motivated Soldiers on CWB's staff rose to the challenge. It turns out, disciplined Soldiers are actually more likely to exercise initiative, because they understand their left and right limits.

As a company commander, I tackle my to-do list only through delegation, a commonality I share with all of my staff section leads. As a unit that is literally always on the move, we're constantly sending small crews of junior officers and junior enlisted out to get

Continued on page 46

Mutual Trust in the Competition Phase of Conflict

By Capt. Adam P. Schinder, company commander, Alpha Company, 915th Cyber Warfare Battalion

Today, the United States is engaged in various levels of international conflict that touches every aspect of the multi-domain battle. While hostile action remains a persistent reality, leadership at every echelon of military and civilian service have identified the value of competition prior to the exchange of lethal fire. Pursuant to this acknowledgment is the charge to Commanders and service members to do all they can to exploit opportunities short of conflict, as allowed by ethics. Failure to do so will adversely affect the frequency, complexity, and length of hostile actions demanded during conflict. In order to fully capitalize on the often fleeting opportunities that exist in this space, now more than ever military leaders must build trust in creative ways with as many partners as possible. In the 915th Cyber Warfare Battalion (CWB), we are internalizing this charge to the best of our abilities; to empower subordinate leaders to make decisions, rather than seek permission. Within the Commander's intent, Soldiers of the 915th CWB are engaged in building trust within the Cyber Mission Force, with adjacent units, with Army Service Component Commands, and with supported maneuver Commands in order to capitalize on opportunities, shape future conflict, and prepare for deployment in support of armed conflict.

I don't believe it is a coincidence that "competence" is listed as the first of the seven key principles of Mission Command as outlined in ADP 6-0. Competency is the cornerstone on which mutual trust is established, enables subordinates to have the proper intuition for disciplined initiative, and offers Commanders a foundation for informed risk acceptance. Every title 10 action in Cyberspace that the Cyber Mission Force is a direct product of deliberate training, demonstrated proficiency, and careful observation of the supported Command's intent and rules of engagement. The 915th CWB activated the first line Company and Expeditionary CEMA Team 1 (ECT-1) with this in mind, and is taking measures to ensure competence is institutionally enforced. The Command has directed all Soldiers in ECT-1 to be aligned against established work roles, providing a technical

Continued on page 51

***FORT GORDON, Ga.** – Soldiers of Expeditionary CEMA Team 1, A Company, 915 Cyber Warfare Battalion, prepare a proximal access device during crew collective training at Training Area 24, January 15 (U.S. Army courtesy photo)*

Relationships Matter: Perspectives from the Platoon Leaders of HHC

By Capt. Aaron R. Bishop, Commander, Headquarters & Headquarters Company, 780th Military Intelligence Bde. (Cyber)

Headquarters & Headquarters Company (HHC), 780th Military Intelligence Brigade (Cyber) is a diverse organization which employs a wide variety of Soldiers and Civilians in numerous technical and administrative roles. The company implements a platoon structure to streamline administrative processes at the company level, and to provide leadership opportunities to junior officers and senior NCOs. As such, these leaders need to balance the administrative needs of the company with the operational needs of their respective staff elements. Mutual trust is crucial to meeting commander's intent, and company leadership often has two (or more) bosses to please. Following is a synopsis of perspectives from the platoon leaders of HHC on how they juggle a complex working environment.

1st Lt. Mason Adam serves as a Cyber Planner in the Brigade's S3 section and as the 2nd Platoon Leader, with responsibility over the S1, S2, and S4 sections. He offers the following perspective:

> *"The diverse backgrounds of the Soldiers, Civilians, and Contractors of HHC/780th working in many different staff sections creates a unique problem for Platoon leadership. The platoon structure is a fitting solution to the natural divisions presented by the reality of staff life. By providing a forum to work as a team to members of differing staff sections who otherwise might not interact, HHC leadership builds mutual trust between themselves and members of a diverse staff. Through these newfound relationships, the members of HHC have more support from their chain of command than before. Utilizing the bilateral relationships across the staff sections, the platoon leadership can more easily meet the intent of the HHC Commander without detracting from the operational effectiveness of their respective staff sections."*

1st Lt. Allan Baily serves as a Cyber Planner in the Brigade's S3 section and as the 1st Platoon leader with responsibility over the Command Group, HHC Orderly Room, Supply, and specialty sections. He has the following to say:

> *"With the OPCON/ADCON relationship, a prevalent theme and issue in the cyber command structure, the same permeates down to companies and the platoons that reside within them. In HHC there are operational goals that the staff sections need to accomplish to support mission success, and administrative requirements at the HHC Company to do the same. Balancing the needs of these two demands as a platoon leader really boils down to understanding both your OPCON and ADCON commander's intent and how that is supported by mutual trust for both sides of the house. Creating a foundation of trust in both avenues allows both leadership chains to understand how the OPCON/ADCON relationship and the desire to support missions aren't mutually exclusive. As a platoon leader I think it has been important to foster relationships with people to build trust in order to tackle commander's intent while trying to balance the fact that many of the Soldiers in the platoon have significantly higher rank and experience. We are fortunate that in HHC we don't have a strong bifurcation in OPCON/ADCON responsibilities and Soldiers understand both requirements. Without understanding commander's intent and mutual trust, though, even simple tasks such as ensuring staff sections complete their 350-1 training would become exceedingly difficult."*

1st Lt. Jeffrey Garcia serves as the 3rd Platoon leader in HHC. In addition to his daily duties, he is

Continued on page 50

Hastati 7 says Take Your Hands Out of Your Pockets

By 1st Sgt. Stanley Collins, Headquarters & Headquarters Company, 780th Military Intelligence Bde. (Cyber)

Four of the US Military Services have active regulations against Service Members putting their hands in their pockets. I am sure Space Force will be on board when they have their uniform regulation. Why is this so important though? Why would every military organization have something in regulation about keeping your hands out of your pockets? The answers seem to be right there in the regulations.

The Army does it so everyone can see we "live by a common standard and uphold order and discipline." (AR 670-1) The Marines Corps does it to "present the best possible image at all times and continue to set the standard for appearance." (MCO 1004.1) The Navy does it to "present a proud and professional appearance that will reflect positively on the individual, the Navy and the United States." (Uniform Regulations Article 1101.3) The Air Force does it "because our three big brothers do it, and our brothers are cool." (citation needed)

While that last line is hilarious, it's barely a joke. Of course the Air Force does this because all the other services do it. The Army, Marines Corps, and Navy have been around longer and have regulations and policies that have made us the greatest standing military in the history of the world. We set the standard of appearance, bearing, and discipline for them and they achieved air superiority in every conflict.

Keeping our hands out of our pockets shows everyone around us we have made a lifestyle choice to be more disciplined than what is the social norm. We will strive to have our behavior, demeanor, appearance, and professionalism to be above that of the average. It shows we have dedicated at least part of our lives to something greater than ourselves that has the capability to change the world for the better. I sincerely believe that service to our nation, whether in uniform or as a Civilian or Contractor is something undoubtedly good. We answer a higher calling. We represent all the best things about the United States. We are all examples that everyone is capable of something greater. We are the example for teamwork completing even the greatest task. Everyone looking and behaving according to the same guidelines is the baseline of this example.

When someone sees us taking care of the little things, it makes it easier for them to believe that we will take care of the big things. This seemingly small thing act can have a massive effect on others. If I see another NCO making a correction, I know that they have what it takes to hold people to a standard. I feel I can rely on them to take care of their platoons, squads, and sections. When I see a leader walk into a section and people start doing the right thing, it tells me that leader will enforce standards and people know it. It tells me people respect that leader and understand what they embody. That leaders knows and enforces standards. That all being said, the opposite is true as well.

When people see our unit, I want them to know immediately that we are professionals. People dedicated to a common goal. They should see we know the details matter. They should see a team dedicated to mission accomplishment by EVERY means necessary. A team answering a higher calling. I want to leave no doubt that we live by a common standard and uphold military order and discipline, in all aspects of the mission and in all aspects of our lives. I want to them to see the pride we take in defending freedom and the American way of life. I want them to see we can be trusted with things that are sacred. I want them to see our hands.

Unit Ministry Team

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

Dave Ramsey, the nationally known financial counselor and radio talk show host puts it this way in his Financial Peace University course, "If you managed money for 'You, Incorporated' the way you manage money for you now, would You hire you?" We live in the self-help and Do-It-Yourself generation. As an enthusiastic and dedicated DIYer myself, I fully understand the appeal of the money savings and the satisfaction received from tackling a difficult job yourself. I must, however, acknowledge that I am an amateur and the results I achieve are not always the greatest despite lots of YouTube help. This is not a major problem when it comes to something like cooking my own meal, painting my walls or unclogging my sink. When, however, it is something of more critical importance and with dire consequences if done wrong, I would be prudent to seek qualified help. It is here that I see many people run into trouble by not using consistent logic in determining who is qualified for the job at hand. If we were in need of dental work, we seek out a qualified dentist. If your transmission goes out, you would want a qualified mechanic. However, there are many other important areas where most people, including myself, are content with "hiring" unqualified applicants.

In the area of finances, one where bad management may mean the loss of hundreds of thousands in retirement savings, we often put ourselves in the place of financial manager, or worse, we don't hire one at all. In the Army we have even less of an excuse as financial management services are a free part of our benefits through Army Community Service. Managing our finances takes not only head knowledge but impulse control. Hiring a bank in the form of a direct deposit to our investment account is a smart move for those of us that find it hard not to put our money straight into our wallets.

Another area that requires impulse control is fitness and nutrition. I have discovered that I, like many people, am not well qualified manage this area. I foresee the need to hire a fitness coach or enlist an accountability partner when retirement puts an end to the motivating bi-annual Army Physical Fitness Test requirement.

Unfortunately in the Unit Ministry Team we often see many people that have hired the wrong person to be in charge of their emotional well-being. This is often a young person who just entered in to a marriage relationship. The person's spouse probably did not even know they were interviewing to manage the other's emotional fulfillment and are woefully unqualified to do so but yet, that is the job they have been given. Structured communication is very helpful to let couples learn how to emotionally support each other. A counselor or some kind of marriage enrichment program should be utilized. Often the attitude that "they should just know" or "we can handle this ourselves" leads to many troubles and sometimes divorce.

No article by the Unit Ministry Team would be complete with speaking about spiritual fulfillment. This is one area that has seen a major growth in do-it-yourself approaches. Our constitutional right to free exercise of religion has placed the Army Chaplaincy in our units to give easy access to qualified spiritual guidance. While this resource may not be for everyone, there is someone infinitely qualified to manage this area of our lives, God.

Mutual Trust, Commander's Intent, and the Lawyer's Take

By Capt. Martine A. Mastriani, Command Judge Advocate, 782nd Military Intelligence Battalion (Cyber)

A successful unit operates with the expectation that each member, regardless of rank, is an effective contributor as a leader and as a subject matter expert. When a commander sets that expectation and holds those accountable who fall below that standard, a culture is formed. In that culture, mutual trust is the point of convergence. Mutual trust that each member has done his part to perform competently helps to ensure the inner workings of the unit function like a well-oiled machine. In turn, this allows the commander to put forth his intent, which is routinely backed by and rooted in sound policy and guidance that cannot be questioned or undermined.

Specifically for the lawyer, the charge is to provide sound guidance on both law and policy to support the commander in shaping his intent before it is ever disseminated. In doing so, the lawyer must be proactive by practicing preventative law during the shaping process. Being proactive rather than reactive creates a more efficient process and eliminates unnecessary back and forth in regards to what can actually be done after the commander's intent is already formed. Therefore, members of the unit are confident that their commander's intent was formed by first seeking counsel by those subordinates and partners surrounding him even though they will not see the process of behind the scenes trial and error. The commander also trusts that the foundation of his intent is impenetrable because those who shape it are always accountable, honest, and educated in their input. Therefore, even in the face of the most dangerous course of action, a commander can make a "clear and concise expression of the purpose of the operation" and his staff will follow suit and execute as professionals.

Further, most of this process is completely unknown to the civilian world. Regardless, the military is still charged with maintaining trust and confidence across the civilian population it serves. Mutual trust is the principle that spans across civilian and military realms. In our case, most of what is done in cyberspace happens in the shadows. While the law, policy, and guidance given greatly depends on the commander and mission, the pillar of principled counsel remains. The lawyer must always operate honestly and transparently. The lawyer is responsible for clearly articulating legal left and right limits, but also advising on policy that will affect the civilian population. The analysis and guidance does not stop at "is it legally sound." The next question will always be "but is it a good idea?" Presenting the commander with the law and potential second and third order effects helps assess whether the anticipated risk is something the commander can or is willing to assume. Lawyers also operate with the understanding that cyberspace is continuously evolving and law and policy are lagging. Guidance changes quickly making continuous, honest communication key. Regardless of echelon or mission, a commander should never have to retract intent because it is unsound, impossible, illegal, or unethical for others to follow. That is a distinct failure and immediately rescinds the mutual trust that was built for both the unit and civilian world. Ideally, an effective staff supports and enables the commander before intent is ever formed. Then, when the commander's intent is disseminated, all members of the unit can and will execute because of mutual trust.

FORT GORDON, Ga. *– The Chaplain (Maj.) Peter Baek (left), chaplain for the 780th Military Intelligence (MI) Brigade, stands with the 782nd MI Battalion Unit Ministry Team, Chap. (Capt.) Jeffrey Brannen, and recently promoted, Sgt. Daniel Gallegos, religious affairs specialist. (U.S. Army photo)*

Why I Stay...In the Fight!

Sgt. Stephen Paradis, Cyber Solutions Development, 781st Military Intelligence Battalion (Cyber) Vanguard!

MOS: 17C – Cyber Operations Specialist

Hometown: Pensacola, Florida

"I started out in college and I didn't feel very fulfilled with how my life was going. My grandfather had been in the Army and he suggested I look into what the Army could do for me. I decided I wanted a purpose and a direction, and that is why I joined the Army."

ON WHY HE SELECTED CYBER:

"I had always been interested in computers from a young age. I knew I always wanted to go into a job where I could work with computers, and when I learned about what the Army was doing with cyber I knew that is where I wanted to be. There were so many jobs and so many different paths I could take in the field of cyber, and the Army was making them available to me. It was an opportunity that I couldn't turn down."

ON WHY HE RECENTLY REENLISTED:

"I spent a lot of time weighing my options, trying to decide what was best for me. In the end I decided to reenlist, not just because I wanted to be a better Soldier or a better NCO (noncommissioned officer), but because I knew that being in the Army would help me to become a better person."

FORT GEORGE G. MEADE, Md. *-- Sgt. Stephen Paradis is a Cyberspace Operations Specialist (Military Occupational Specialty 17C) assigned to Cyber Solutions Development, 781st Military Intelligence Battalion (Cyber), Fort George G. Meade, Md. (U.S. Army photo by Master Sgt. Cory MacNeil)*

ON HIS FUTURE GOALS:

"One of my short-term goals is to become the certified as Senior Developer so that I can lead other Army software developers and create a team that will become the "go-to" team for the difficult projects no one else wants to do. My biggest long-term goal is to become a subject-matter expert on multiple different coding languages and technologies so that I become one of the Army developers that people come to when they need questions answered."

ON WHO INSPIRES HIM:

"My hero and my inspiration is my grandpa. Throughout my life he has always been a strong figure and he has always lived by the Army Values – even after he got out. In doing that, he taught me what was right and what was wrong, and I grew up with a role model who always helped me go in the right direction."

HIS FAVORITE QUOTE:

"Great goals make great people. People cannot hit what they do not aim for." – Roy Bennett

PRAETORIANS

780th MI BDE
"STRENGTH AND HONOR"

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

U.S.ARMY

President's Cup Cybersecurity Competition

WASHINGTON -- *An all-Army team was awarded top accolades at the first government-wide President's Cup Cybersecurity Competition hosted by the Cybersecurity and Infrastructure Security Agency.*

Army Chief Warrant Officer Three Benjamin Koontz, technical advisor for DISA's Cyber Operations Directorate, along with Army Major Josh Rykowski, Army Cyber Command; Chief Warrant Officer Four Phillip Smith, 781st Military Intelligence Battalion; Army Sergeant First Class Zachary McElory, and Army Staff Sergeant Matthew Cundari, both of Army Cyber Protection Brigade, took first place in the competition.

Over 1,000 individuals and more than 200 teams of federal employees and military members competed in the competition, which began in September and was comprised of three rounds, with the final taking place Dec. 11-13. Contestants—both individuals and teams—took part in the first two rounds remotely by solving Jeopardy-style Cyber challenges in a virtual environment. (Courtesy photos)

Information Warfare and Army Public Affairs

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

I recently read an article on the *Defense One* website "Should the U.S. Have a Secretary For Influence Operations?" As I read through the article about influence operations and the various disciplines associated with Information Warfare – cyberspace, electronic warfare (EW), information operations (IO), psychological operations (PSYOP), and tactical signals intelligence operations – I kept asking myself "What about Army Public Affairs?"

The potential transformation of Army Cyber Command (ARCYBER) to Information Warfare Command would be a significant change in narrative for an Army headquarters, beneath United States Cyber Command, with operational control over Network Enterprise Technology Command (NETCOM), 1st Information Operations Command (Land), Cyber Protection Brigade, and the 780th Military Intelligence (MI) Brigade (Cyber).

One of my duties as the Army public affairs officer for the 780th MI Bde., the U.S. Army's only offensive cyber brigade, is to scour the internet for any open-source intelligence that has an impact on my organization, to include reports from the traditional news media, defense and cyber-related publications, blogs, and research from cybersecurity companies such as FireEye and Cisco Talos.

The 780th MI Bde. is a major subordinate command under ARCYBER and any information relevant to information warfare – ICEWS (Intelligence, Cyber, Electronic Warfare, and Space); the 915th Cyber Warfare Battalion (CWB) and its associated ARCYBER pilot program CSCB (Cyberspace Electromagnetic Activities (CEMA) Support to Corps and Below); and our Nation's adversaries and their information warfare capabilities – which has an effect on my organization is what I 'pull and share' with the command in order to keep them informed.

On March 13, Lt. Gen. Stephen Fogarty, commanding general, ARCYBER, was addressing Army Signal leaders and industry at AFCEA's 2019 Army Signal Conference in Springfield, Virginia, when he was paraphrased as stating that "the future success of the military was the domination of information. The integration of cyber, electronic warfare and information operations is a fundamental aspect of this success."

Fogarty went on to say, "It's this idea that whoever can sense, understand, decide and act faster than the adversary enjoys the decisive advantage."

Gen. Fogarty's position on the proposed ARCYBER transformation to Information Warfare Command is shared by the Army Chief of Staff (CSA), Gen. James McConville, who was recently said ARCYBER "is an ideal spot for future military influence operations because it's in a position to extract potentially relevant digital information, surveying the digital landscape of the target operation, and delivering cyber effects…"

As alluded to in the article, the intent of the CSA in establishing an Information Warfare Command is "a need to counter disinformation on the ground in places where U.S. forces are already doing business," and this was where I asked "What about Army Public Affairs?"

Army Public Affairs professionals should have a role in an Information Warfare Command, be integrated into the CSCB pilot, and a part of the ICEWS and 915 CWB organization.

As background, I started my Army career in Armor, deployed in support of Operation Desert Shield/Storm, was branch transferred to Ordnance, and spent the last 18 years of my active duty career as a Public Affairs Officer (PAO). I served an operational tour in Kosovo in 1999, served two tours in Iraq and a tour in Afghanistan and part of my duties as the command's subject matter expert for public affairs was working with intelligence, operations, IO, civil affairs, and PSYOP staff officers and sections, the Staff Judge Advocate (SJA), and the kinetic/non-kinetic Fire and Effects Cell, to advise them and the command on how to best incorporate the public affairs discipline into operations and engagements in order to achieve the commander's goals and the associated measurable actions.

A caveat, in order to be successful in supporting

information warfare I believe public affairs professionals need to: remember who they work for; show their value to their command; and understand public affairs actions/inactions will shape the narrative.

I served as the 4th Infantry Division (4ID) PAO and primary spokesperson for Multi-National Division-Baghdad (MND-B) during Operation Iraqi Freedom Rotation 07-09, and a critical point I repeatedly made to the brigade PAOs was they work for their respective commanders. The public affairs program is **the** commander's program. Ultimately, the commander is responsible for everything that happens (and doesn't happen) in their command and the PAO is an advisor.

Their job is to be a public affairs SME, know their organic capabilities and what capabilities are available to them, to become a valued member of the command, a contributor, and someone who has a seat at the table.

Another point I made to the brigade PAOs was, by nature of our business, when we engage the news media, our communities, and our internal audience (Soldiers, Army Civilians, Veterans and their Families), and external audience: we shape the narrative through our actions and inactions (i.e. community partnerships, speaking engagements, press releases, articles, social media posts, access).

Understandably, there is a huge debate in the public affairs (PA) careerfield on whether or not PA should be involved in influence operations and how closely should we work with Information Operations (IO). I would argue that everything PAOs and their respective organizations 'do or don't do' influences our publics. It's not that our primary objective is to "influence" them, moreso we shape their opinion and position by providing them with facts, answering their questions, and when something cannot be stated due to operational security or privacy concerns, telling them so – most people get it.

Army Public Affairs is the primary conduit between our Service and our internal and external audiences and we accomplish this through a variety of mediums and platforms. When I was an PA instructor at the Defense Information School, I told my students their only limitation was their imagination. If done correctly, along with others within the organization, we identify our key publics, we determine how they ingest their information, we understand the commander's intent, and then we use all our internal and external capabilities and assets to do our part in ensuring mission success.

When I was in Iraq, the 4ID and MND-B division commander told me my primary focus was the Pan-Arab and Iraq news media. His reasoning was the U.S. and Western news media would come to us if they needed a story, but the conduit to the Iraqi people and those in the region were the news mediums they got their information from. Understandably, there are news outlets in the region that are more digestible to the Shia populace and those watched more by Sunnis – think about how some Americans gravitate toward Fox News or CNN.

Daily, my staff and I would go through the U.S. and Westerns news reports, and we had Arabic translators going through Pan-Arab and Iraqi news reports. The purpose was two-fold, to see if our messages were resonating and to look for misinformation. As we scoured the news, my team was looking for any reports on our operations and of the Iraqi Security Forces and its government. Those reports were reviewed and researched through operations and intelligence to gauge its validity, and if we identified there was misinformation – there was a process in place to combat it in a timely fashion.

A caveat. As with any organization, there is going to be bad news and the one thing I was taught early on

Continued on page 52

***BAGHDAD** — Iraqi Gen. Abud Qanbar, and Maj. Gen. Jeff Hammond, commanding general, 4th Infantry Division, and Multi-National Division-Baghdad, at an Iraqi/Western Media press conference at FOB Prosperity. (U.S. Army Photo)*

A Nibble on Mutual Trust and... (cont.)

Continued from page 6

- With implementation of the Assignment Interactive Module, empowerment of the Soldier to have an active role in assignments will be of great benefit to encouraging Soldiers to make the Army a career as it facilitates involvement in the process

Throughout the process of deciding to accept the Army as a career, is the element of leadership. Oftentimes, a Soldier will say, "They did this, they denied that, or they decided something that affected them in some fashion." Rest assured, the "they" can be generalized as leadership from the top to the bottom. Each leader impacts career decisions on a daily basis. So, how do we become better leaders? Study and observation of current and past leaders is one way. There are also a number of publications that focus on military leadership; each method has its own merit and place. However, I want to highlight a 1943 publication I recently became aware of, "Psychology for the Fighting Man". It is an interesting read overall that provides some early insight into what Soldiers thought regarding what makes a good leader (p372-388).

A leader then, to be worthy in the eyes of his men would do well to follow these commands:

1. Be competent.
2. Be loyal to your men as well as to your country and Army.
3. Know your men, understand them, love them, be proud of them.
4. Accept responsibility and give clear, decisive orders.
5. Teach your men by putting them through the necessary action.
6. Give only necessary orders, but—
7. Get things done.
8. Be fair.
9. Work hard.
10. Remember that a leader is a symbol. Men need to respect and trust you—don't let them down.

The following is a summarization of a Soldier survey that highlighted what was considered the core elements of good leadership; all of which hold true today.

- Ability – competence comes first
- Interest in Soldier welfare
- Promptness in decision making
- Good teacher/instructor
- Judgment/common-sense
- Does not "boss you around"
- Recognizes good work and compliments Soldiers on their work
- Physical strength and conditioning
- Good education/sense of humor/courage
- Impartiality – fair across the board
- Industry – work as hard/harder than the Soldiers
- Clear orders

By applying these tested principles, leaders can foster an environment of mutual trust and influence personnel to transition from job to career-mindedness. Leadership is not an easy endeavor and takes dedication to get it right. Good leaders strengthen the Army by creating an environment that encourages its Soldiers to strive to be the best they can be which also influences individual decisions to choose the Army as a career when they have other options. I can attest to the value of good leadership as it was a critical component in my decision making regarding whether or not to Stay Army at several points in my career. Please take a moment to consider your role in Soldier's decision-making process – you are the difference.

References:

Psychology For the Fighting Man : Prepared For the Fighting Man Himself / By a Committee Of the National Research Council, with the Collaboration Of Science (p372-p384)

https://babel.hathitrust.org/cgi/pt?id=mdp.39015031512521&view=1up&seq=388

PRAETORIANS

780th MI BDE

"STRENGTH AND HONOR"

DET-HI -- Mutual Trust and Commander's Intent (cont.)

Continued from page 31

from higher, the shared vision for the organization, and perspective; your trust in your command team is the key to success. Conversely, the trust you are given means that within the framework of Mission Command, you own the mission, have the authority to make decisions, and take risks based on your perspective and understanding of the Commander's vision and what will ensure mission success.

As I finally depart this fine organization, I am experiencing a mixture of emotions: Pride as the Brigade continues to grow in both capability and capacity, solidify its identity, and my Brothers and Sisters in Arms (virtual) make the vision reality. Nostalgia as I look back at where we started, the hard work, the fun, and the frustrations at turning a commander's vision into the only Offensive Cyber Operations unit in the Army. Excitement at leaving the Brigade and heading to the next chapter, taking with me all the lessons I've learned from all of you Cyber Warriors, and looking forward to showing my future command team that I trust them and that they in turn can trust me to accomplish every task, without fail.

DET-TX -- ...in a Joint, interagency environment (cont.)

Continued from page 32

General Mattis clearly conveys how important he believes trust and commander's intent are to good leadership and mission success; his message can and should be directly applied to the Cyber Mission Force. Commanders should encourage initiative and trust their subordinates to continue on mission without constant oversight. Leaders then should be ready to take a commanders intent and find the best way to their end-state.

The Cyber Mission Force will continue to grow in the years to come. Trust across all Services will be a key factor in our future success. Trust up and down the chain of command will affect how the Cyber Mission Force reacts to new threats tomorrow. Commander's intent and the tenants of Mission Command will allow leaders at all levels, as General Mattis stated, to "unleash their initiative". The future will hold many obstacles for the Cyber Mission Force, but by working together, we can find the solutions the mission requires.

"Light the Way, Through the Dark"

HHC/915 CWB -- Developing a Culture of Military Discipline (cont.)

Continued from page 35

things done with some minor direction and intent. Our forward logistics elements, cyberspace planners, and expeditionary cyber operators are proving every day that they can make on-the-spot decisions with the guidance they've been given from their chain of command and execute such decisions with confidence and conviction. If CWB is going to plan for and operate at the "tactical edge" then its Soldiers need to fully understand the commander's intent, know their left and right limits, and confidently take initiative to exploit operational success.

Several studies have observed the relationship between autonomy and productivity. Increased autonomy at work has been linked to increased retention rates, increased employee productivity, and decreased stress among employees. Stressors can be classified as those over which we do and do not have control. The more control we feel over our stressors, the easier it is to manage and work to overcome the negative emotions that come with stress. Giving Soldiers increased autonomy to handle specific aspects of their day encourages them to work harder towards the things they can control and accept the things that they can (or should) not.

The bottom line is that autonomy and discipline are not antonyms. A Soldier can be a disciplined member of a team who is capable of making autonomous decisions that support the commander's intent and the team's overall success. For any organization that relies on creative, motivated hard chargers to accomplish the mission, success hinders on leadership's ability to foster a disciplined environment that values individual initiative.

782nd MI: Cyber Warriors, Cohesive Teams (cont.)

Continued from page 28

have been here doing this much longer. Despite the 7th Cavalry's victory at the Battle of the Washita River, this was not the case at the Battle of Little Bighorn.

When looking at building cohesive teams through mutual trust, it is clear that Custer did not trust his junior leaders at the Battle of Little Bighorn and in turn did not foster a positive and productive environment. There were multiple occasions where Custer would revoke or rescind previous orders given by his junior leaders; often making decisions that were illogical or arbitrary. This showed us that Custer had very little trust in his junior leaders, specifically in this case with Maj. Marcus Albert Reno, his second in command. Custer frequently questioned his junior leaders' ability to make good decisions and would repeatedly reverse or change the orders originally given by his subordinates. This further created an environment of distrust and disloyalty. Countless scriptures and historical documentation showed that Reno disliked Custer and it was clear that the dislike of Custer was shared among many of his junior and senior officers.

When Custer first made contact with the enemy near the valley of the Little Bighorn River, his scouts accurately reported to him that the enemy numbered in the 7000's, with at least 2000 of them being comprised of the fighting age warriors. Custer's force only numbered at about 500 men. He was outnumbered by at least 4 to 1. Despite these reports, Custer did not believe he was facing that large of a force. He himself even rode to the top of a mountain called the Crow's Nest where the scouts were overlooking a portion of the enemy, but still he could not effectively see the enemy situation. Due to terrain limitations from this point of view, he could have only seen about ten percent of the valley that held the Indian villages. He dismissed the scouts' reports and created a false understanding of the enemy situation and failed to share this information with his subordinate commanders. This is a perfect example of how Custer failed to build mutual trust by sharing information and relying on council of his subordinates. Had he done so, they might have been able to convince him to heed the warnings of the scouts and avoid splitting his forces.

Sometimes in cyber we want to rush to success. We don't create a shared understanding of a very hard target set. We don't effectively train our Soldiers, and we don't listen to our scouts that have seen the enemy before. To be successful we must lean on our NCO Corps to train our Soldiers without being dependent on outside agencies. If Soldiers are not trained, they lose confidence in their own ability, and begin to lose trust and respect for the leaders that don't provide them with what they need to be successful.

Why Custer developed an environment of distrust is not very well understood by historians. It could be since individuals like Maj. Reno and Capt. Frederick William Benteen (third in command) had proven to be ineffective officers and often disagreed with Custer or maybe because Custer felt his ways of doing things were better and led his men directly rather than delegating. Custer was also known to be a leader who gave very vague orders without ensuring his men understood his intent. During battle, Custer often found his men executing his orders not at all in the way he envisioned. If Custer would have provided clearer guidance and expressed his intent, battle outcomes could have been very different as junior leaders could have felt empowered to exercise discipline initiative.

Custer was now beginning his attack. He decided to split the regiment into three separate commands. Captain Benteen was ordered to scout to the west with three companies. Major Reno was ordered to attack up the valley with three companies and press the enemy northward. General Custer told Reno, "Take your battalion to try and overtake and bring them to battle, and I will support you." After visiting the Crow's Nest Mountain, General Custer changed his mind and decided he was going to move northward through the bluffs to the east with the remaining five companies, and attack the enemy from the flank. Clear orders were given, but clear intent was not. Furthermore, he changed the plan and did not get word to Major Reno about the change. There is no evidence that there was a clearly defined end state that Custer wanted to achieve as a tactical maneuver task. This left his two other units without

a clear understanding of the intent of the overall mission, and proved fatal for many in Major Reno's command.

We would argue our current orders process in cyber needs work. We have yet to see a full five paragraph OPORD describing the enemy situation, left and right units on the battlefield, clear intent of what the overall mission is, etc. Yes, we have mission plans but we just don't think that gets after covering all the bases. Lack of clearly defined orders further creates lack of trust.

Having thus received orders, Major Reno attacked up the valley and was stopped cold by the enemy. He then ordered his men to dismount and to form a skirmish line instead of continuing the charge to the north, which is what we are led to believe Custer wanted him to do by most sources on the matter. Major Reno was then attacked by several hundred of the enemy. He became confused and did not give clear orders to his men, which resulted in a rout of his command that fled to a nearby wooded area and subsequently to the top of the bluffs to the north, fighting for their lives every step of the way. Without clear intent from Custer, Major Reno was left with indecisive instructions and could only attempt save himself and his men.

Captain Benteen executed his mission by moving to the south through very rough terrain that slowed his progress. He had no idea of Custer's intent, and was just doing as he was specifically ordered. Once Custer made contact with the enemy and realized their size, he sent word to Benteen to come quickly and to bring the pack trains. Benteen did not come quickly, but instead dawdled. There was no explanation of intent of the situation and Benteen did not realize that Major Reno and General Custer were decisively engaged until he met up with Major Reno's command on top of the bluffs. The lack of clear mission intent greatly contributed to Captain Benteen and Major Reno's lack of understanding of what Custer was trying to accomplish. Had Custer fully explained and possibly even rehearsed the plan, the outcome of the battle might have been much different.

A cohesive team is critical to success as a team, and mutual trust is critical to a cohesive team. Custer did not have a cohesive team. His subordinates were individually motivated by their own ideas and agendas largely because of his failure to unite them with a mutual understanding. In cyber we need to all be united in making our branch work. We need to be motivated by our sense of patriotism and comradery, and not just by our paychecks. Lack of training can create a lack of trust, and immature decisions amongst our younger cyber warriors. With our current situation in cyber, Soldiers have been promised extra pay for being a part of cyber. We as leaders must do everything, we can to ensure we process cyber assignment incentive pay.

We can learn many good and bad lessons from the Battle of Little Bighorn but one of the most important is that Soldiers should always come first. Their wellbeing, understanding of mission, and most importantly, trust in leaders and peers alike is paramount, because as we have seen in history repeatedly, without trust, there is no victory. Most of what we do (technically) is not very well understood even by some of the most distinguished and successful leaders within our organizations. This is likely due to the complexity and intricacy of our work, combined with leaders' lack of experience and technical understanding in the cyber domain, all within a rapidly changing environment. The challenge is to mitigate this by building trust. Today's leaders must not make the same mistakes made by past leaders like General Custer. We must build trust, trust within each other to accomplish objectives, trust in the advice and council given by Soldiers, and trust that leaders will make sound and logical decisions. It is our responsibility as leaders and Soldiers to embrace all the principals of mutual trust and build cohesive teams in order to ensure mission success. Of the 586 Soldiers, 31 Officers, 33 Indian scouts, and 20 Army Civilians at the Battle of Bighorn, 268 were killed in action, including General Custer, and 68 were wounded.

This horrible lack of mutual trust and cohesive teamwork rendered the 7th Cavalry combat ineffective. Hopefully we can all create relationships of mutual trust and avoid a "Cyber Little Bighorn".

Cyber Trafalgar (cont.)

Continued from page 34

where all other ships could observe and take commands from his signaleer. The signaleer would relay commands through the movement of flags while subordinate commanders would maneuver their ships based on the commander's instructions. In other words, the commander was the puppet master, and the ships of his element were his marionettes.

As Lord Nelson constructed his plan of attack against Villenueve, he knew that Villenueve's fleet relied heavily on the direction of their commander. He knew that splitting the Franco-Spanish fleet, and depriving the separated elements the instruction of their puppet master would cause confusion amongst the ranks. This confusion could serve as an advantage on Lord Nelson's behalf under one condition. His men had to be ready to operate without his direction during battle as well. Conducting a perpendicular attack against the Franco-Spanish fleet would cause his fleet to also become decentralized and unable to take direction from the commander's ship. Lord Nelson understood that success in battle would be reliant on accomplishing two critical goals. First, he had to ensure that his subordinate leaders understood the plan of attack unequivocally, and second, he had to trust in the ability of his subordinate leaders to execute his plan without the need for his instruction during battle. In other words, he relied on mutual trust between himself and his men. He would attain mutual trust through scrupulous planning and preparation. Lord Nelson went over his battle plans with his subordinate leaders ad-nauseam. His planning and preparation was so meticulous that there was no doubt in his mind that his men could execute the battle plan without the need for a puppeteer's strings. In other words, he developed a clear shared understanding amongst the leaders and Sailors of his fleet. Lord Nelson was not ignorant to the fact that his plans were not all perfect. He understood that error and deviations were a possibility. This, however, is where his trust in the ability of his men took precedence. Although Lord Nelson was known to outline every possible outcome of a battle to a minutia's detail, his plans still allowed for the flexibility of subordinate leaders to react decisively to changes or deviations in the plan.

Meticulous planning, proper preparation, the ability to properly execute a plan, and the ability to react decisively to changes in the plan are all important attributes that any team preparing for an operation should embody. Meticulous planning and preparation is especially important when operating in a dynamic and complex environment like that of Cyberspace. Cyberspace is a domain where a single bit offset, or a rounding error in the hundred-thousandths decimal place, could lead to catastrophic failures in a critical system. The success of a mission in cyberspace lie in having a deep understanding of the systems that make up the area of operations. It may be far-fetched to believe that someone can understand everything about even one component of an entire system. That said, this logic is not an excuse to forgo making the attempt to do so. Failure to understand as much as possible prior to conducting operations in cyberspace will only increase the probability of failure through missing a critical aspect that could later cause problems. Lord Nelson did not go over every possible outcome of the Battle of Trafalgar with his fleet leadership prior to the operation. It was his ability to identify what was important and ensuring the he went over as much as he could in the time allotted to him that made him successful. Likewise, the more a team conducting cyberspace operations are efficient in their preparation, and work to understand the systems in their area of operations, the smaller the chance of missing the minute detail that an adversary can exploit.

With meticulous planning and preparation comes the trust leaders need to allow their subordinates to conduct their respective tasks without the requirement of detailed instructions every step of the way. Due to the time sensitive, extensive, and complex nature of Cyberspace, successful operations in this environment require agility. Agility is achieved when each member of a team has a deep understanding of their respective function, and each member of said team can effectively and efficiently integrate their functions into the collective function(s) of the team. When a leader can focus on maneuvering his force as a whole, and not on giving detailed instructions to individual members of his team, the unit is agile and able to better adapt to the quick and ever-changing situations. This was the case with Lord Nelson in the Battle of Trafalgar.

Continued on the next page

Continued from the previous page

His plan depended on the fact that his subordinate leaders could function and operate when the fleet was separated and decentralized. He had great confidence in his men. Similarly, any element conducting operations in Cyberspace will see success if two things occur. First, each individual member of a team must master their respective function and be able to operate within the parameters of this function with minimal guidance. Second, the leader of a team must understand how to properly employ the capabilities of his team to achieve the desired effects necessary to accomplish the team's mission.

Although the Battle of Trafalgar ended as a tactical victory for the British, the victory had strategic effects in the Napoleonic War. It was this battle that not only helped solidify the dominance of the British Navy for generations beyond the Napoleonic War, but also crippled the combat power of the Spanish forces leaving their navy all but destroyed for the remainder of the war. Lord Nelson and his fleet used ingenuity, effective planning and preparation, and fine subordinate leadership to defeat the larger and more equipped Franco-Spanish fleet they faced. Lord Nelson, his fleet, and all the variables that contributed to his successes in the Battle of Trafalgar serve as critical lessons learned for the future battles that will be fought in the seas of cyberspace. Achieving tactical dominance in cyberspace will be highly dependent on outside-the-box thinking and ingenuity, proper planning and preparation, and mission command.

Platoon Leaders of HHC (cont.)

Continued from page 37

responsible for the readiness of the Brigade's robust S3 section. He has the following to add:

> *"There is no duty more sacred in the Army than leading Soldiers. Being a Platoon Leader is the best opportunity for a junior Officer to have a direct and tangible impact on the lives of Soldiers and DA Civilians. I have the distinct privilege to see my people every day, enable them to do the mission they signed up to do, and be an advocate for them when they need one. Accomplishing the missions of HHC and my tech-ops team is a balancing act. It starts with the intent of my leaders. The rest of the articles in this edition will talk about what commander's intent is and why it matters – I won't belabor that point. But I will emphasize that intent is the sandbox that I work in as a junior leader. I can do whatever I need to, within its boundaries, to accomplish my commanders' intents so long as they trust me to do it.*
>
> *Gaining trust is like replacing an engine block: it isn't complicated work, but it is a lot. I gain the trust of my teams and bosses by being present. When my soldiers have to do something that sucks, I make sure that I am there. When my commander or section OIC needs something done, I make sure it happens. And I show my people that I care about them by taking an interest in their lives and genuinely getting to know them. These basic things are no secret to any leader, but even former Secretary of Defense Mattis preaches "brilliance in the basics". That in mind, effectively balancing differing intents takes good delegation. I have trust in the NCOs, Warrants, and Officers on my team and in my Platoon to effectively carry out the tasks that I need them to do, and they trust me to ensure what we are doing adds value and makes sense. When the commanders' intents pull in different directions, I leverage the people in my elements to accomplish everything that needs to be done. In this way, the mutual trust between myself and my subordinates allows me to build mutual trust between myself and my leaders."*

A common thread that my platoon leaders touch on is the building of relationships and teams. A senior leader once stressed to me that relationships matter, and nowhere else in a battalion than HHC is this more important. On a day-to-day basis, the success of my command is dictated by the relationships we garner in HHC and the trust that we build. Having served in three HHC's prior to taking command here, I've noticed the best commanders I've ever had were the ones that fostered teams, and who took the time to build relationships across all echelons.

Mutual Trust in the Competition Phase (cont.)

Continued from page 36

foundation for incoming personnel to receive training parity with the rest of the Cyber Mission Force. This offers Battalion leadership the freedom to employ forces to conduct title 10 cyberspace action while we work out the requirements specific to expeditionary information warfare operations. At the same time, 915th CWB in conjunction with the Cyber Center of Excellence are designing individual and collective qualification tables with Training and Evaluation Outlines that capture tactical as well as technical competencies. Finally, competency is being built through the shared experience of Soldiers employed on tours in the Joint Mission Operations Center, with supported maneuver Commands, and thru overseas deployments. These actions are ongoing in the pursuit of building mutual trust across the Cyber Mission Force and building ECTs prepared to earn the trust of supported Commands.

FORT GORDON, Ga. *– (left to right) Sgt. Breyon Samuel and Sgt. Alexander Lecea are graded by Staff Sgt. Robert Vickery during a "Call for Fire" evaluation during Tactical Training at Training Area 29, November 22. (U.S. Army courtesy photo)*

Military formations do not operate unilaterally, particularly in the context of competition below armed conflict. This in mind, 915th CWB deployed leaders to USARPAC (U.S. Army Pacific) and USAREUR (U.S. Army Europe) to engage with their Commands and staffs to discuss their operational initiatives, current challenges, and how the CWB could be employed. Following these initial interactions by the Brigade and Battalion leadership, ECT-1's Team leadership and junior leaders were empowered to build mutual trust and begin problem solving with their staffs. The Commands engaged with ECT-1's leadership, worked-out the particulars of expeditionary CEMA support to their current operations, and have employed the operators of ECT-1 to carry out those actions. In support of their actions, the Battalion and Company are feverishly resourcing and training the ECT, while writing the processes to continue outfitting future ECTs.

It is an exciting time to be a part of offensive cyberspace operations in the United States Army, and in particular the 915th Cyber Warfare Battalion. We owe a debt of gratitude to the foundational work of our predecessors in the 780th Military Intelligence Brigade (Cyber) and the Cyber Mission Force. Through continued partnership, exchange of talent across the force, and collaborative planning efforts with supported Commands the 915th Cyber Warfare Battalion is cultivating the requisite trust needed to support the nuanced objectives of conflict below armed conflict. At the same time, the Battalion's continued engagements in Decisive Action Training Environment with Brigade Combat Teams is preparing the ECT to fight and win in war as well. In January and February, our Soldiers maneuvered with 1 / 3 ABCT (1st Armored Brigade Combat Team, 3rd Infantry Division) during their collective live fire at the National Training Center, trained to certify in their work roles, and planned for future operations across the globe. All this work is done in the pursuit of mutual trust with whom we support and to expand the trust needed for more complex expeditionary information warfare operations.

Information Warfare and Army Public Affairs (cont.)

Continued from page 44

in my PA career was *"You can't shine a turd. You can polish it, gold plate it, but at the end of the day, it's still a turd."* It's best to admit your mistakes, to own and address them, and in these cases, you need to get the command and staff (operations, intelligence, SJA, and host-nation advisor) involved.

One of the tools an effective PAO should have is a network of reporters to contact in the event something is egregious enough to warrant an engagement. In Iraq, this meant taking the time to translate the information in order to push it out through the Pan-Arab and Iraqi press. This could entail not only U.S. and western media briefings, but those for the Pan-Arab and Iraqi press as well. It is all about building and maintaining a relationship with reporters and that takes time, trust and credibility.

I am clearly on the side of a very close relationship with those involved in information warfare with a HUGE caveat. Trust and credibility are two traits an effective PAO must build and maintain with the news media and the community. Once lost, I would argue the PAO needs to look for another career. A PAO should not be a source of information if they are involved in deception operations.

Actually, I don't recommend involving your PA assets in any deception operation. The moment they lose the trust of the news media their credibility is gone, and in the long run, I believe that hurts the Army Public Affairs career field and the credibility of the Armed Forces.

Furthermore, when a brigade's public affairs primary focus, during training center rotations, is on getting stories back to their home station, they are doing their commands and the Army a disservice. If it's a requirement to inform the home station Families and community, then plan for the division or training center public affairs staff to do this mission. I believe public affairs should have a larger role in information warfare and be a part of the planning, training and execution process.

One last point, there is a difference between an FA 30 (information operations) officer and an FA 46 (public affairs). Based on experience, I argue that IO can use the products of public affairs to support their operations, but the PAO should be extremely wary of using any IO product. They should be separate entities and not work for one or the other

Don't get me wrong, I am a big proponent of IO. In Iraq, my staff and I were right next to the IO section. Each week, along with the civil affairs team, we briefed the MND-B Assistant Deputy Commanding General for Support on our operations to ensure we were in sync and executing the commander's intent, but only rarely did I use IO products. An example of when I did use IO (PSYOP) products were the leaflet drops referencing Jaysh al-Mahdi (JAM) thugs who were operating throughout Baghdad in 2008. The JAM were criminals, terrorists, murderers, and we passed out leaflets on the JAM lieutenants during press events and used them as a boiler plate on Pan-Arab and Iraqi news releases. Why? They were bad people, wanted for doing very bad things to their own people, and it was effective.

In closing, I believe Army Public Affairs can and should be a part of information warfare and as the Army moves forward on potentially transforming ARCYBER to Information Warfare Command, and building the ICEWS units in support of the combatant commands in the Pacific and Europe, I hope they ask themselves – "What about Army Public Affairs?"

FORT GEORGE G. MEADE, MD. *— The 780th Military Intelligence Brigade (Cyber) Praetorian EZ-Up shelter is put to good use at the Meade Express; sheltering our Soldiers pulling duty during the COVID-19 pandemic. (U.S. Army Photo)*

"STRENGTH AND HONOR"

780TH MILITARY INTELLIGENCE BRIGADE

In the next issue:

* 780 MI Brigade Commander Exit Interview
* 780 MI Brigade Change of Command