780th MILITARY INTELLIGENCE BRIGADE (CYBER)

THE BYTE

Vol. 9, Issue 1

The Army Civilian:

BUILDING THE FUTURE THROUGH CHANGE

780th MI BDE
"STRENGTH AND HONOR"

Col. Matthew Lennox
Commander
Command Sgt. Maj. Ronald Krause
Command Sergeant Major

780th MILITARY INTELLIGENCE BRIGADE (CYBER), Fort George G. Meade, Maryland, publishes The BYTE as an official command information publication, authorized under the provisions of AR 360-1, to serve its Soldiers, Civilians, and Families.

Opinions expressed herein do not necessarily represent those of 780th MI BDE or 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.

Send articles, story ideas, photographs, and inquiries to the 780th MI Brigade (Cyber) Public Affairs Officer (PAO) and The BYTE Editor, Steven Stover at steven.p.stover.civ@mail.mil, or mail to 310 Chamberlin Avenue, Fort George G. Meade, MD 20755, or call (301) 833-6430.

On the Cover
FORT GEORGE G. MEADE, Md. – *Joint Military Operations Center (JMOC), 780th Military Intelligence Brigade (Cyber)*

THIS ISSUE OF THE BYTE magazine is focused on the Brigade's Army Civilian work force and the theme is "Building the Future through Change." Greg Platt, the Brigade's Senior Cyber Advisor, stated "change will impact the organization whether we acknowledge it or not. Effective organizations must evolve to meet the needs of future requirements." Platt challenged the Army Civilians throughout the organization to submit an article describing how their organization, or the 'Information Advantage' enterprise in general, must evolve to be successful.

Also, in this issue of The BYTE, U.S. Army Cyber Command's newest command, the 915th Cyber Warfare Battalion, conducted a Field Training Exercise at Muscatatuck Urban Training Center in early October 2020 and Soldiers from the Army's first Expeditionary CEMA (cyberspace electromagnetic activities) Team, ECT-01, were the target audience. ECT-01 is the first of 12 ECTs, and early next year "The Harbingers" will activate their second (Bravo) company.

Building the Future Through Change

By Gregory A. Platt, Senior Cyber Advisor, 780th Military Intelligence Brigade (Cyber)

WHAT IS IT ABOUT CHANGE that makes people uncomfortable? You would think in our environment we would be accustomed to change, as it seems it is an everyday part of our work life. The truth is most people resist change out of fear of the uncertainty that is inherent with change. Research from UC Berkeley suggests our brains are wired to perceive ambiguity or uncertainty as a threat. To counter this threat, we naturally try to gather relevant information to reduce the uncertainty and thereby eliminate the threat. If our data gathering efforts don't satisfy our needs, we tend to get anxious and stress out.

We will continue to evolve as an organization and changes will occur in the near future. Hopefully, you are not feeling anxious and stressed out over these changes. However, if you are, here are a few things you can personally do to improve your ability to cope with the pending changes.

Practice Acceptance. As the old prayer goes "God, grant me the serenity to accept the things I cannot change; the courage to change the things I can; and the wisdom to know the difference." Acceptance allows us to move forward rather than being stuck in a cycle of resistance and frustration.

Reject passivity. Don't sit back and wait for things to happen. Actively engage with leaders to gain insights into the impending changes and seek ways to assist in the implementation.

Maintain Positivity. Keep a positive outlook and perspective. Trust that our unit leaders have your interests and mission success as central elements of any organizational change.

Significant organizational changes that will affect our workforce in the near future:

CP71: The realignment of portions of our Cyber Effects workforce into CP71 is complete. Over the coming year we will continue to refine the professional development program offered by CP 71 so that we can receive maximum benefit from their offerings. You can leverage the new CP to your advantage by ensuring you have a valid, meaningful and up to date Individual Development Plan.

Cyber Mission Force workrole rebalance: The Brigade has completed adjustments to our organizational structures to meet the new Cyber Mission Force requirements. The workrole, MOS (military occupational specialties) and grade changes will be published in an out of cycle FY22 TDA (Tables of Distribution and Allowances). The rebalance impacted the number of civilian EAs, IONs and other types of analysts on the team, but the total number of civilians remained the same. In other words, no positions were decremented based on this rebalance effort.

Realignment to U.S. Army Cyber Command (ARCYBER): While the timeline for this transition isn't fixed, there is ongoing coordination between ARCYBER and U.S. Army Intelligence and Security Command (INSCOM) to have the Brigade service aligned to ARCYBER. Current coordination indicates the Brigade will optimistically transfer under ARCYBER sometime in FY22.

Establishment of an ARCYBER aligned Military Intelligence Group (MIG): INSCOM and ARCYBER are coordinating the establishment of a new MIG. The Georgia based MIG is intended to provide direct support intelligence collection and analysis support to ARCYBER. While many of the resources required to support the manning of this new organization will be competed for at the Army level, ARCYBER G2 and 780th MI Brigade will provide resources to help establish the its initial operating capacity. 780th is currently designated to provide 33 billets (mixture of MIL/CIV). The resources will likely begin to transfer sometime in FY22.

Transition to Cyber Excepted Service (CES). The Army will begin to utilize the personnel system known as CES in FY23. While there is some school of thought that 780th would be a good candidate to transition to this new personnel system, especially after transition to ARCYBER, there are currently no definitive plans to do so.

Reference:

- https://greatergood.berkeley.edu/article/item/seven_ways_to_cope_with_uncertainty

SHOUT OUT TO EXCELLENCE

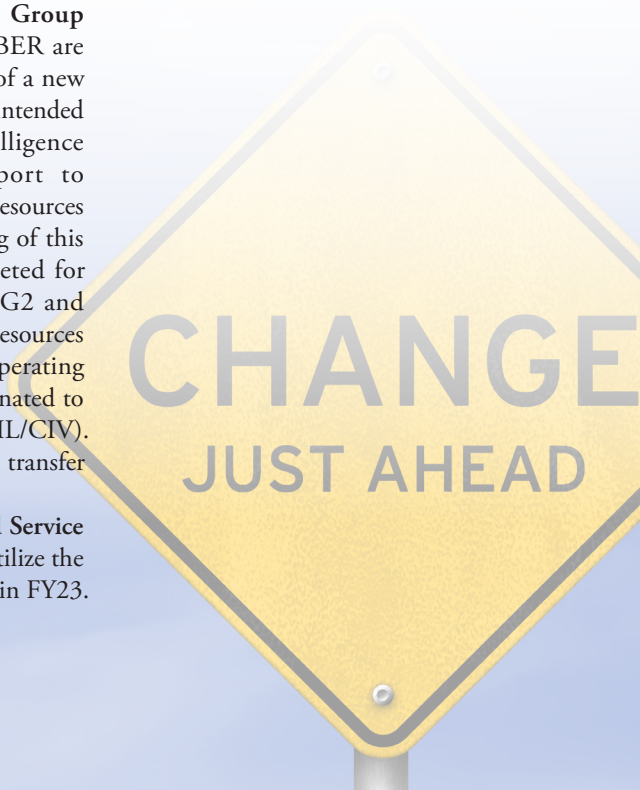
Connor Shade: *First to solve last Quarter's Warrant Officer Challenge*

Cheryl Smith: *INSCOM OPSEC Award*

Lucas Holmbeck: *Task Force Employee of the Quarter*

Outgoing CWC Representative: *Steve Lim*

New CWC Reps: *Toni Pisciotta, Matthew Ellis, Nancy Taylor*



Courage in the Face of Change

By Craig Morris, Deputy Chief of Planning, 780th Military Intelligence Brigade (Cyber)

"*We cannot expect success fighting tomorrow's conflicts with yesterday's thinking, yesterday's weapons or yesterday's equipment.*" – Former Secretary of Defense James N. Mattis in front of the Senate Armed Services Committee, April 26, 2018

THE IDEA THAT THE POWER of the American war machine is most effective by studying the lessons of the past and adapting them to win the wars of the future is nothing new to warfighting professionals. Applying antiquated methods and capabilities that are out of sync with our adversaries' capacities can quickly steer the ship off course in its journey to fulfill our national security objectives. Why then, do our leaders rely on out-of-date venues, technologies, and exercise scenarios when training to fight future wars?

This question was weighing heavily on my mind a couple of months ago on September 11th as I was driving to work on my normal daily commute. Like many people, this mundane morning ritual often offers a much-needed time of reflection for current events and the impacts of significant moments in history and their protracted effects on our daily routines. In the case of 9/11, to call the impact of these events on our society 'profound,' is an understatement. Nowhere is this more relevant than in the Department of Defense – specifically within the intelligence arena and, by proxy, the cyberspace warfighting domain. The methods by which members of our community trained for and fought wars forever changed on that horrific morning in 2001.

Despite the vast amounts of American treasure sacrificed on the battlefields of Iraq, Afghanistan, and Syria over those years, the silver lining is that the lessons we learned from our successes and failures defending the acts of that day, ensured American global dominance for the following two decades. But after 19 years of a counter-insurgency-themed wartime-footing, the time has come for America to forge forward with new methods, venues, scenarios and capabilities and prepare ourselves for tomorrow's war, the war we KNOW will be different from any war of our past, and set conditions to be in the best place possible to win it before it ever begins.

Of course, we all know these truths, so why then is it so hard to change direction and train differently; to respond to enemy actions differently; to seek new venues and build new tools, new teams, and new methodologies that offer different and challenging perspectives of our government's role in maintaining global security? The answer is often FEAR. Fear of change and the unknown; fear of failure and its consequence; fear of exposing unit deficiencies; fear of displaying individual ineptitudes resulting from inadequate training pipelines; fear of ostracism by subordinates, peers, and seniors; and ultimately the fear of escaping from what's comfortable – from that oft-derided mundane.

The solution to overcoming these fears, thankfully, is in our own hands. In our role as steadfast civilian leaders within the Army cyberspace team, it is imperative that we create a work environment where change and innovation is commended rather than condemned; where failing fast is encouraged rather than admonished; where empowering junior leaders to make decisions at the lowest levels and conceive new methods of tradecraft without fear of reprisal. For it is they who are most in tune with the emerging worlds' paradigm of power. In fact, now is the time we need to fail, in modernized training environments where the risks are still relatively low, not in the face of the next competing superpower with the fate of our national security at stake.

Too often we resort to harboring environments linked directly to successes of our past, filled with processes and procedures that won wars that we will never fight again. We press the "easy button," and "stick with what worked" instead of making ourselves and our teams vulnerable by introducing elements of the unknown. Not vulnerable in a negative sense, rather in a positive one, by creating new opportunities to learn and progress as a unit, as an institution, and as a community. Our advancement, and a guarantee of preparedness, depends on it.

In order to give ourselves the greatest opportunity for success, we must change the way we prepare. To paraphrase General Custer – we cannot overestimate our ability to win by resting on our laurels. We have been fortunate over the years to have held the edge over our adversaries by maintaining state of the art equipment, technology, and training regimes. We must continue to shape that success through persistent development, reimagining our

Continued on page 3

Continued from page 2

adversaries' capacities, and ensuring our technological advancements keep up with our individual demands of increased data availability in our training and operational platforms. The time has come to embrace creative destruction, to archive our comfortable-ness and re-envision our aging military industrial complex to better suit the demands of cyberspace.

As we begin a new chapter in the Army's years-long initiative to create a civilian cyberspace effects career program, the opportunity is ripe to take a fresh look at our tenured tactics, techniques, and procedures and wipe the slate clean to create the most modern and effective cyber workforce on the planet. Fear has no place in this equation; now is the time for courage. Courage to stand up for what we know needs changing. Courage to take on the workload of improvement. Courage to transform the way we train into the way we will need to fight to be successful in tomorrow's wars. Nothing worth fighting for is easy, but knowing that the benefit of American exceptionalism extends both domestically and internationally, the act of courage to achieve it becomes less so an idea than a requirement.

To achieve the successes our nation requires, we cannot continue to train in and for the "post 9/11" counterinsurgency environment of the past two decades. We must rely on the ingenuity of our youth and provide an open and free-thinking work environment that encourages change, emphasizes fast-failure and growth, builds upon perceived unit-level and individual deficiencies, challenges the aging training pipelines and venues we've grown comfortable with, and erases any sense of ostracism from coworkers, regardless of hierarchy. We hold the power to ensure our continued greatness on a global scale, and it is up to us to achieve it! ■

~~Civilian~~ Leadership in a Cyber World

By Roy Luongo, Director, Joint Mission Operations Center, 780th Military Intelligence Brigade (Cyber)

SO FOR THOSE OF YOU THAT don't know me outside of my current role, I came from here. I came from the roots of the Brigade. I came from a time of about 40 individuals in the backrooms over on the "main compound" of the infamous "Det Meade". We were a bit ragtagged and we all thought we had the digital world by tail. And then we grew, and grew, and branched off, developed ASIs (Additional Skills Identifier) and MOSs (Military Occupational Specialties) and Branches. I am not saying we were the sole entities involved, but I like to see us as a 'nucleus that divided and split'. In addition, many of us came back as Civilians or contractors after we finished our service. Why did so many comeback? That is a personal answer for each of them, but I guarantee you, none of them came back because they had nowhere else to go (queue Richard Gere voice).

So why did I decide to come back? I'll wave my flag a bit here, because there truly was a sense of ownership and pride in seeing what Cyber had become and where it was going. When I retired the Army Network Warfare Battalion had just unfurled. Later, I left the government and went to the corporate world for a few years. However, the sense of purpose was missing for me. That is a personal feeling, not to begrudge all the fine people who leave government, but I was missing the impact of what we do.

I came back to the Brigade and the Joint Mission Operations Center as it was about to explode into its mission space. It was a great time to come back in my opinion.

Obviously, there is a significant difference coming into a predominantly military organization as a civilian. First, how do we fit into the organizational structure? Where are our authorities and responsibilities aligned? Do we have authority? We definitely have responsibilities. I will say I was impressed with the level of education on the topic that is available to us as civilians. Even though some is mandated, I encourage everyone to take advantage of the CES (Civilian Education System) opportunities. I am not going to dive down the doctrine on being an Army civilian, mainly because I am not an expert, but the one thing that is apparent is we are the continuity, we are the professionals who bridge PCS/ETS, change of commands, etc.

So how do we manage, work with, work for and team build with our military coworkers? First, you need to define who you are in the context. I am not discussing some metaphysical awaking, but I am talking about understanding your role, your knowledge, your GAPS, and how those come together with the mission you are assigned to. Our position descriptions are a start, but we all know they can be lacking. Meetings with our supervisor to discuss expectations is a must and team build and mission level setting round out the basics, but then there is the challenge of understanding the soft skills and the implied task of our jobs. Those are learned over time and practiced to refine.

So how does a Civilian lead in a military organization? It can be tough, and I promise you at some point in your tenure you will hear, "I don't work for you" or "You're not my rater" and that individual will absolutely be correct. Often we are leading without authority or utilizing positional authority versus general military authority and that may be the hardest challenge for prior service members. That form of leadership is often harder and requires more intra-personnel skills and conflict management than the traditional (and in some cases antiqued) direct, knife-hand style of leadership. I remember my first experience with Civilian leadership shortly after my retirement and I was cautioned by my first line supervisor that I had to talk nicer to Civilians. It's a little tongue and cheek now, because we should always talk nicely to each other, but it was a learning curve of those intra-personal skills that don't always come easy to old crusty NCOs. You don't want to even know the laughs I got when I needed "work-life" balance explained to me.

My first recommendation as a leader is to develop a leadership philosophy. Even if you are not a leader yet, develop how you want to lead if or when given the opportunity. Your general philosophy will adjust depending on the mission you are leading, but define your core tenets and the type of leader you want to be.

My approach to leading in a military organization is what I call "be the least significant bit." For those not into the geekdom, the least significant bit is rightmost bit in a byte string. It is the one with the least impact on a given byte if changed. Some people find this counterintuitive to a leader's role, but hear me out. It doesn't mean I am the least essential, although at times that is true. It does not mean I cut myself out of the planning cycles or decision processes. I define it as ensuring in the absence of my direction the organization will still function, because of the goals and vision that are set. Develop your organization so that you aren't the smartest person at the table. Your input may add to the outcome, but surround yourself with those that have even higher value input to the team.

Steve Jobs said, "it doesn't make sense to hire smart people and tell them what to do; we hire smart people so they can tell us what to do." John Wooden (NCAA basketball couch) said, "Whatever you do in life, surround yourself with smart people who'll argue with you". I strive for both. Part of any good MDMP (military decision making process) session has COA development and COA Analysis. If your team is not empowered to go left and right to develop COAs or they are

Continued on page 5

Continued from page 4

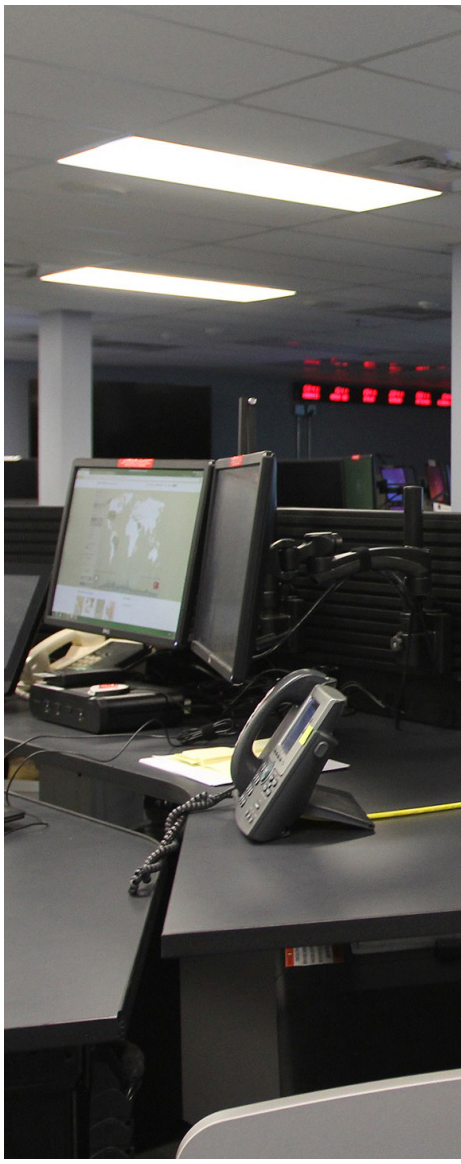
uncomfortable telling you your COA has flaws during analysis you are hamstringing your organization. End every meeting with "What did I miss?" and truly accept the responses.

As a Civilian leader, we need to understand how to manage both Soldiers and Civilians. I find it more challenging on the administrative side than on the operational side. The operational side is fairly simple for me. There is not difference. The job performance I expect from a Soldier is the same job performance I expect for a Civilian. There should be no difference in expectation. The positions within my organizations, for the most part, are not designated military or Civilian and the JQS (Joint Qualification Standard) is not different for one or the other. The administrative side has a lot of differences and that is the largest learning curve in my opinion. As prior service, I understood the military structure and administrative needs, in the most part. Somethings have changed, but 4187s are 4187s and leave forms are leave forms. The Civilian side was new to me. Time sheets, IDPs (Individual Development Plan), performance plans and review, were all new to me, but the Army came to the rescue, they have courses, documents, and SOPs for that. Although, understanding the nuances of maintaining a Civilian work force is challenging, knowing what Civilians can or cannot be required to do, how hours and all the various hourly codes work (or don't work) is daunting at first. I love what I do, but paperwork and "administrivia" is brutal. I call it my "tax" for being a part of a mission I love. And we as leader should pay our "taxes" and learn to take care of our Civilian work force as well as we take care of our Soldiers.

That leads into the next leadership challenge. How do we develop a force while doing our mission? This is increasingly hard in a mission set that has no down time. Old Combat Arms models were one team operational, one team ready, and one team recovering. This model does not work in 24/7/365 optempo. There is no down time. Yet, we have to find time to train our team. Train them in the specifics of their mission. This tends to be technical, and should be no different in how a Civilian or a Soldier is trained. The standard is the standard. Look at your organization and have training paths for work roles that can be tailored to individuals based off feedback from your SMEs (back to Jobs and Wooden). Have a training plan and have multiple courses of action to achieve that plan. In Cyber we demand a deep technical understanding of our technologies and that comes at a price of both time and money. It is an investment we are willing to make, but we cannot always maintain. So for every in-person lecture or hands on class you identify, look for alternatives if you can't acquire that training and identify how you can fill those gaps with OJT and mentoring.

Development is a different focus. In development, we are educating our workforce for the next thing. We need to understand what the individual wants to do, an honest assessment of what they have the aptitude to do, and your ability as leader to facilitate that education and broadening. I encourage you to look at your personnel and challenge them both vertically, opportunities above their current skillset, and horizontally, opportunities to the left and right of their current mission set. If someone wants to become a leader in the future, challenge him or her with leading small working groups or tiger team projects. If they want to become a digital forensic analyst, see if you can flex their time to shadow someone in the forensic section. This is a scary thing for many leaders, because there is risk. To truly do this you must trust the individual, but also give them the room to fail, but this often means the potential to you failing as something that is your responsibility (remember that thing you can never delegate). That's our burden as a leader, to take that risk. It will be ok, just give it a shot. One of the hardest challenges to individual development is that we as leaders must become comfortable with developing someone "out" of the organization. Know the goals and 5-year plans of your Civilian team members and you MUST help them accomplish those even if it means moving out of the organization. You will lose great people, but as a strategic leader, remember someone else is gaining a great person.

In line with that, you have to develop the team as a collective unit. There are very limited functions in an organization that are not truly collective. The summation of the individual's tasks is an amalgamation of those tasks into the collective task, not just a grouping of serially completed items. This is incredibly difficult in a 24/7 operations center and often I find myself having to rely on an assessment of ongoing mission versus a true VALEX posture. Regardless, you have to be able to identify those collective efforts and be able to practice them. Just like with the



***FORT GEORGE G. MEADE, Md.** – Joint Brigade (Cyber)*

individual, you need to stress your teams to build the resilience and strength in their collaboration.

Lastly, self-development and assessment (remember least significant bit). Be a forever learner, a continuing education junkie. I challenge you to look at it more abstractly then just take a class or get a degree (although I highly encourage those activities). How else can you learn? Well, put yourself in areas of increased responsibility or opportunity. Find a working group or extracurricular function that builds your knowledge set. If you cannot take time to go to formal training, can you provide training or mentoring? In my current position, I do not get near a keyboard nearly enough, but I teach externally as an adjunct professor and instructor. That keeps me knowledgeable in the technologies we employ. This harkens back to not being the smart person in the room, but I have to be able to understand and work with the smartest person in the room. I will let them fight over who that is.

So in summation, being a Civilian leader in a military organization can be a challenge, but it is worth it. If you come from a military background learn how the civilian workforce functions, understand the nuances between the two. Develop the soft skills of leading without authority. Develop your leadership style and strive to live it. Continually develop and challenge your team members, the team, and yourself. And know you are making a difference every day. When I look back at the legacy of "The Det" and future in front of ARCYBER (U.S. Army Cyber Command) I am proud to be a small part of it. ■

Military Operations Center (JMOC) U.S. Army Intelligence and Security Command (INSCOM), 780th Military Intelligence

Brigade Army Civilian Receives Award for Superior OPSEC Program

780th Military Intelligence Brigade (Cyber)

FORT GEORGE G. MEADE, MD. – Cheryl Smith, the brigade's OPSEC (Operations Security) officer for the 780th Military Intelligence Brigade (Cyber), received the U.S. Army Intelligence and Security Command (INSCOM) OPSEC Program Individual Achievement award for 2018 in a ceremony at the brigade headquarters, November 11. According to Ricky Eden, the brigade S3 CUOPS (current operations) supervisor, the award is a significant achievement considering INSCOM has 19 major subordinate commands and more than 17,000 employees. Smith was selected over other award nominees because she constructed a "superior OPSEC program" for a geographically dispersed brigade with more than 1,350 Soldiers, Civilians, and contractors assigned to brigade subordinate headquarters in four different states and with elements outside the continental U.S. (OCONUS). In the award justification memo, the brigade S3 CUOPS wrote "The brigade's OPSEC Officer, Ms. Cheryl Smith maintained awareness and oversight of the overall brigade and subordinate units' OPSEC program activities and was the first face encountered on the subject of operations security. She provided initial face to face training to all newly assigned personnel and personally trained over 230 Soldiers, Civilians, and Contractors in the calendar year 2018. Her training provided an overview of current threats, both CONUS and OCONUS, unit vulnerabilities, critical information, and most importantly their responsibility to the Brigade's mission as well as operational standards and the Army Values."

Additionally, Smith provided guidance, inspection schedules, and other pertinent program information to 32 OPSEC representatives within the brigade. She ensured OPSEC appointment orders for all subordinate units were updated and that OPSEC Level 2 Training was completed by all primary and alternate OPSEC Program Managers.

"Whether on duty or off duty, everyone is responsible for the information in their possession," said Smith. "OPSEC everyone's responsibility."

FORT GEORGE G. MEADE, Md. *– Cheryl Smith, the brigade's OPSEC (Operations Security) officer for the 780th Military Intelligence Brigade (Cyber), received the U.S. Army Intelligence and Security Command (INSCOM) OPSEC Program Individual Achievement award for 2018.*

Leading Organizational Change Through Culture Change

By Pedro Santiago-Gonzalez, Senior Civilian Advisor, 781st Military Intelligence Battalion (Cyber)

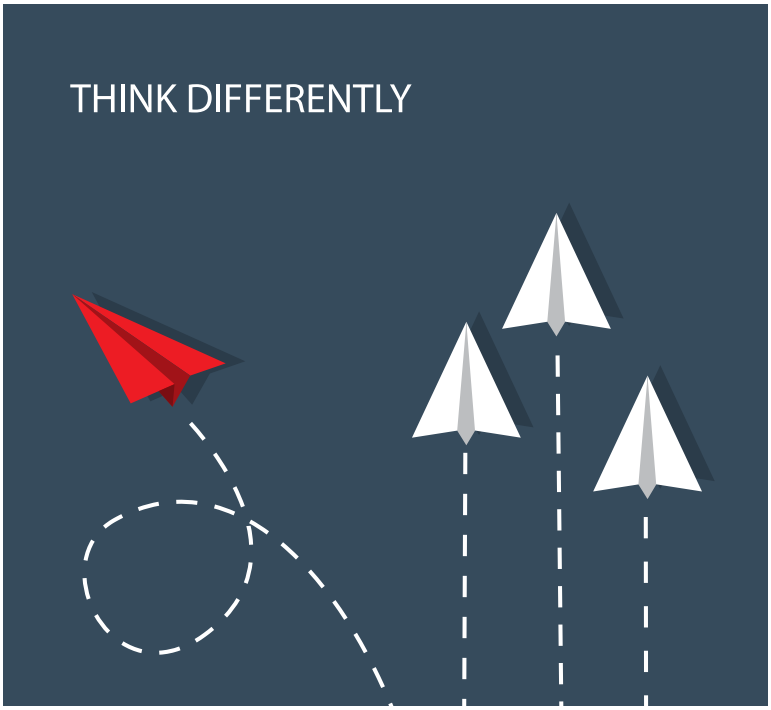
CHANGE IS INHERENTLY A DIFFICULT thing to do when we as humans are used to learning and then get used to routines and often get comfortable in our ways. Change is difficult for some individuals but much easier for others. Why is that? What makes one accept change and go in a different direction without hesitation or reservation. I believe it's up to organizational leadership to set the tone of one's organization's culture; lead by example and execute. I wholeheartedly believe that if an organization's culture has been established, created to be inclusive to everyone, open to constructive criticism and have the ability to pivot towards progressive culture and inclusiveness, we can drive positive changes in the workforce.

This starts at the top of any organization. The culture is set by leaders at all levels but it starts with the leadership at the top. Leaders have to establish goals, values and aspirations that everyone can achieve. Whether these aspirations are personal or professional. We as leaders need to create pathways for individuals to achieve personal and professional greatness. We achieve this by first and foremost treating those around you the way you want to be treated. This goes a long way in establishing trust between your employee population and key leaders within the organization. The next action is to have more face to face organizational events. These can be leader professional development (LPDs), team bonding events and/or command sponsored events. These events allow those who generally work in remote spaces to come together for an event to mingle, converse and often time vent. We need more events that bring team members.

Leaders need to be approachable, no matter the circumstance. A real open door policy allows fellow team members the confidence to step forward and have frank and honest conversations on various issues within the organization. These don't always need to "issues" these can also be highlighting the positive/ good that is happening within the organization. Leaders need to be visible to the workforce. Leaders need to step out of the mundane routine and circulate throughout all work spaces, make sure that team members see them and interact with them. This gives them a sense that the organization's leadership cares enough to go out of their way to see what they are doing and working on. Leaders need to be inclusive and have transparency on organizational changes. When we make changes, the workforce should know the "why" and "how". They should be tracking that changes need to be made in order to achieve a desired outcome. Whether that is instituting "VANGUARD Time" or expressing the reasons it has been shelved. Small changes make huge differences within an organization. We need to make sure we are making positive changes that will result in a more cohesive and inclusive organization. One that brings pride to being a Department of the Army Civilian within the 781st Military Intelligence Battalion (Cyber).

Why is that? What makes one accept change and go in a different direction without hesitation or reservation.

I am here to create and set a culture that is enduring, that lasts for years to come and to be able to shift in positive ways in order to adapt to the ever changing workforce. I want inclusion and respect for not just for all Civilians but for all officers, Soldiers and warrant officers.



Shaping the Analytic Workforce to Meet Future Challenges

By Victor C. Anderson, A Company, 781st Military Intelligence Battalion (Cyber)

THE DIRECTOR OF NATIONAL INTELLIGENCE has established analytic standards to promote a common set of ethics for achieving analytic rigor and integrity. Agnostic of any specific intelligence discipline, these tradecraft standards seek to address issues of analytic objectivity, bias, politicization, and other issues. These standards have long-reaching effects and also establishes a foundation for education and training in analytic skills and tradecraft.

As technology changes, so changes the craft of intelligence analysis. Almost as soon as a technology is developed, it is used for intelligence purposes. Communications technology advances have had the effect of changing entire societies, with communications and information technology reaching into every aspect of human behavior. It has enabled some countries to bypass several developmental steps and transform themselves virtually overnight from agrarian to information-based economies.

Understanding the technologies involved in the various intelligence disciplines and their strengths and limitations are crucial skills for the intelligence analyst. Analysts must be able to adapt to changing technologies and tools used in their analysis, as well as have a thorough understanding of their adversaries' technologies. An understanding of the technical aspects of signals collection, knowledge of all forms of communications are vital in the performance of these analysts' mission. In technical intelligence disciplines such as ours, it is imperative that analysts remain conversant in emerging technologies which pertain to their disciplines.

In addition to being technically proficient in the skills required for their profession, intelligence analysts must also possess an analytical method of thinking and be sufficiently comfortable with their own thinking processes. Intelligence analysis requires an understanding of the reasoning methods so the analyst understands the nature of his own thought processes in order to challenge his own assumptions. To remain mentally agile and analytically relevant, it is important that analysts are familiar with their own cognitive biases and how to mitigate them, and apply critical thinking techniques to their daily work. Fortunately, these skills can be learned and honed through practice. Additionally, there are cognitive tools, structured analytic techniques (SATs) such as the analysis of competing hypothesis (ACH) which provide a framework for better analytic skills.

In understanding their own methods of reasoning, some terms are useful to the analyst as well. Generally when we talk about reasoning, we are referring to three broad categories:

- **Deductive reasoning** stems from having possession of some, if not all the facts of a situation, then drawing a logical conclusion based on these facts. However, due to the nature of intelligence, the information available to the analyst is often intentionally misleading, incomplete or simply in error. This type of reasoning is generally tautological, relying only on available facts and evidence which may be in error, thus leading to erroneous results.

- **Inductive reasoning** can be seen as the opposite, where few facts are known, general conclusions are drawn from the available information. This is more in the nature of intelligence analysis, where the veracity and completeness of information is suspect, and only available a little at a time. While inductive reasoning can also lead to false conclusions based on incomplete information, it also has the potential to lead to new truths.

- **Abductive reasoning** is the most closely related to the craft of intelligence analysis as the intelligence analyst is never in full possession of the facts. This form of reasoning accepts that information as presented may be incomplete and/or in error. Abductive reasoning makes an educated guess based on the available information and evidence, what the analyst knows of similar situations, and to some degree, intuition and imagination. Abductive reasoning has the advantages of creating working hypotheses which can be challenged and tested, the possibility of discovering new truths from the available information, similar to inductive reasoning, as well as being predictive in nature, which is the essence of the intelligence process.

In practice, intelligence uses all three of these reasoning modes to some greater or lesser extent to arrive at the finished intelligence product, with abductive reasoning being the most relevant to the intelligence environment.

Intelligence analysts must be comfortable with working in an environment where complete facts are never known, and the veracity information available to the analyst is usually suspect to some degree. The analyst must be able to draw conclusions quickly despite these handicaps and most importantly, communicate their findings in a meaningful way to intelligence customers.

The two broad categories of technical

and cognitive skills encompass essentially the entire scope of skills and abilities required for analytical competency. The technical landscape of intelligence analysis will only continue to become more complex. New technical collection and analytical tools emerge almost daily. Tools such as network mapping, database and query tools, and data visualization tools, are vitally important to intelligence analysis especially due to the overwhelming amounts of information available to today's intelligence analyst. It is clearly important that the analyst be computer literate, possess solid researching skills, be sufficiently organized in order to sort through large amounts of information, and formulate effective database queries. However, such skills do not, by themselves, constitute competent analysis. Similarly tools, no matter how capable, are not a panacea. Tools should support and enhance the analytical process but do not, in themselves, provide answers to analytical questions.

Without the ability to accurately discern the meaning of the output of an analytical tool, the information provided can be worse than useless. An analyst's cognitive abilities will determine his ability to think critically, interpret data and determine its validity and relevance to the intelligence need, and ask the appropriate questions of the data. Software tools, analytical techniques, processes, and intelligence organizations do not produce intelligence without the intelligence analyst having the ability to "apply the wetware to the software", i.e. apply analytical reasoning to intelligence information. Further, the analyst must be sufficiently attuned to intelligence customer's needs to determine what information relates to the intelligence question. Most importantly intelligence is useless if no one except the analyst knows about it. The analyst must be able to take complex information and communicate it effectively to customers. ■

Change: Know It. Deal With It.

By Bud Roth, C Company, 781st Military Intelligence Battalion (Cyber)

CHANGE? CHANGE COMES IN MANY FORMS—good, bad, and the inevitable. Change is closely related to the concept of time and the fluid, kinetic nature of reality. There are two broad categories of change: changes we make and changes to the operating environment outside our control. For any organization, successful mission execution requires the ability to not only affect change, but to adapt to external changes that impact operations. Thus, every organization needs a game plan for dealing with change and making sure that mission-essential activities stay on track. This article examines the sorts of change that our Battalion faces and how we might go about handling them.

Types of Change

As the Soldiers and Civilians in 781st Military Intelligence Battalion set our minds to tackling change, it is worthwhile prioritizing and categorizing the changes we face. There are a number of ways to do so. One fundamental way to split change is into "internal change" and "outside change". We will return to the elements of successful internal change later, but first, let's examine some of the outside changes that we have little or no control over:

- **Environmental Change** – The COVID 19 pandemic is a great example of an environmental change that impacts the battalion in a myriad of ways – from changes to target behavior, to workplace restrictions to changes in Internet traffic that might impact operations. Aside from this unusual example, another critical environmental change is change to the Internet, a form of infrastructure change. The cyber domain within which we and our targets operate is owned by neither group, but its contours impact us. Changes in traffic patterns triggered by developments such as content delivery networks ("CDNs") or the rise in government and enterprise cloud operations all change the landscape within which we operate. Russia's efforts to decouple from the greater Internet and China's Great Firewall are two more specific examples of infrastructure developments that impact those contours. Just as infantry must train differently for a beach landing than moving into mountainous terrain, we must understand and be able to navigate the evolving cyber landscape and operate in a variety of cyber environments.
- **Target Change** – Changes in behavior by a target as well as selection of a new target bring a variety of changes that operators must adjust to. An operational organization such as ours must be able to detect and respond to rapidly to a variety of changes in targets. This includes switching to a new computing environment. Examples include moving to a handset for day-to-day computing needs, moving work locations, and connecting to the Internet via a new access method (i.e., traditional TCP networking vs. TCP over 4G). A new target may communicate in a different language or behave in ways dramatically different from previous targets (such as hours of operation and use of social media). Targets' OPSEC (operational security) may change over time too when, for instance, they become more savvy about our TTPs (tactics, techniques and procedures) and activities.
- **Mission Change** – Although leadership is properly considered to be part of the organization, when leaders of an organization approve a radical change to the organization's mission, it requires a dramatic shift in day-to-day activities and organizational structure that impacts the entire workforce. While one might argue that "mission change" is internal change, for the bulk of personnel in an organization, they have no say in how the mission changes, but play a vital role in how that mission change is implemented in terms of day-to-day tasks. In that sense, the big picture "mission change" is akin to an external change and, for simplicity's sake, is treated as "external change" here. It is also worth noting that private sector companies spend a lot of time and money on establishing a corporate vision (desired end state), engineering the company's mission (strategy to reach the desired end state), and defining goals (tactical objectives). This time and money speaks to the fact that understanding where an organization needs to go is challenging.

Filtering Out Irrelevant Change

With all these sorts of changes to track, the task of keeping on top of change is daunting. Where does one begin? The answer to that question is surprisingly simple – although the implementation is not! The question of which changes matter and which changes do not is a critical one and one that cannot be answered by looking at the change in question alone. Instead, the change's impact on battalion operations must be considered. If the change could impede the battalion's ability to execute its mission or, alternatively, open up new opportunities to do the same, that change is significant. So, the question of which change matters can be simply put as:

Does the change in question impact the battalion's ability to carry out its day-to-day operations (now or in the future)?

This impact can be positive or negative, but it is the potential for a change to impact battalion operations that makes external change matter. Change that does not impact us – directly or indirectly – simply does not matter. Sometimes, a change's impact might be indirect. An example of this would be where a new tool enhances our foe's ability to defeat our efforts. Although the tool's existence

Continued on page 12

continued from page 11

does not impact our operations, its use by the foe does. So, the question is simple, but understanding which changes have a potential impact requires a firm understanding of the battalion's mission and that understanding must be present wherever change is encountered. In other words, it must reside in all our personnel. That is the challenge. All of us at every level of the battalion must keep on top of developments that affect us and the organization and each of us must have the ability to recognize when a change threatens to impact the battalion's mission.

2019 CNMF Civilian Performer of the Year: John Moore

By Eric Manthei, B Company, 781st Military Intelligence Battalion (Cyber)

DISGUISED AS A MILD-MANNERED TARGET AREA REPORTER (TAR) for 01National Mission Team (01NMT) and the Cyber National Mission Force (CNMF), John Moore fights a never-ending battle for truth, justice and the American way of life as the CNMF, 2019 Civilian Performer of the year. Some say he is faster than a speeding bullet, more powerful than a locomotive, and able to leap tall buildings in a single bound. With powers and abilities far beyond those of a mortal analyst or reporter.

You may ask yourself, how John achieved CNMF Civilian Performer of the year, and he would say through hard work, and steel like determination to report the SIGINT fact! John started his storied career as a humble private (E1) in the U.S. Army as a 98C in 1997, better known today as a 35N. He served assignments in the 3rd Infantry Division, Fort Stewart, Georgia, 403rd Military Intelligence (MI) Detachment, Misawa, Japan, 704th MI Brigade and Special U.S. Liaison Advisor Korea. John transitioned into the quiet civilian life as an U.S. Intelligence and Security Command (INSCOM) contractor at Fort Belvoir, Virginia, and eventually became an INSCOM civilian where he honed his skill as an Analyst and Reporter. As a TAR, John made significant contributions to the CNMF in 2019 as a certified Adjunct Instructor for RPTG2235, RPTG2318, RPTG4397, and RPTG4398, educating countless CNMF civilians and military members, not to mention other partner agency civilians, the art of reporting. For his tireless effort and outstanding work with the National Cryptologic School in 2019, John received a Letter of Appreciation from the Chief of the College of Cryptology and the Chief of A24. The Cryptologic Chief stated on his award, "John epitomizes learning at its best: keeping up with the latest developments in both the operational and educational realms, infusing operational experiences into his lessons, and promoting knowledge transfer in the workplace among students and colleagues." In-between teaching class, John was able to contribute to 141 reports throughout CNMF, keeping the intelligence community and government officials at the highest level informed. This was just the tip of the iceberg when it came to John's contribution to the Intelligence Community and CNMF in 2019. John assisted in the writing of the TAR JQR at the Basic, Senior and Master level, as a member of the 780th MI Brigade (Cyber) Technical Working Group, which were ultimately adapted by CNMF as the standard for reporters. Based on John's vast knowledge of reporting, he was selected to be the TF1 Senior Reporting Official and aid the CNMF in the Analytic Integrity Standards Review of CNMF reporting. As a member of the review board, he conducted quarterly reviews of CNMF reporting to identify weaknesses and ultimately improve the quality of reporting in CNMF. In addition to contributing as a board member, he taught several brown bag training sessions for CNMF Senior Reporting Officials, increasing the awareness within CNMF. Based on his work on the Standards Board, the Director of Intelligence, CNMF, recognized John with a Certificate of Appreciation for his efforts in ensuring the quality and accuracy of CNMF reporting. John was bestowed yet another honor by being selected as the CNMF Civilian of the Quarter for 3rd quarter FY19, which ultimately led to him being selected as the 2019 CNMF Civilian Performer of the year. You would think John could not possible do more, but you would be wrong! John also served as the Intelligence Oversight (IO) officer for TF1, which received an outstanding score during TF1's IO inspection in 2019. Upon completion, the CNMF Intelligence Oversight Program Manager lauded John's efforts as timely and crucial to the Intelligence Oversight program. I would also be remiss if I did not mention that John assisted TF1/2/4 in completing product phasing, which can be grueling at times, but mandatory to be a fully functioning Task Force, and currently assisting TF5 with their product phasing. John's selfless service, desire to excel, and steadfast attitude to reporting and mission is why John was selected the 2019 CNMF Civilian Performer of the Year.

“SafePayload”

By Cyber Solutions Development Detachment, D Company, 781st Military Intelligence Battalion (Cyber)

CHANGE IS UPON US. IT IS happening around us and it is happening now whether we are active, or even knowing, participants. Even as I write this it is dawn on U.S. Election Day. The voices of the American voter and this Democratic process will have lasting effects on many things including stock prices, taxes, healthcare, the environment, and the future Commander-in-Chief. We likely won't know which path lies ahead for some time, be it days or weeks, but regardless, it will result in change.

New leadership brings new goals and visions for how the organization does and should operate. New personnel bring new outlooks, ideas, and diverse skillsets. New projects often mean learning new techniques and technologies, or adapting old methods in new ways. The COVID-19 pandemic has allowed us to embrace a new paradigm of off-site work that was previously a very foreign concept for many in the Cyber and Intelligence realms. This was probably less significant for the developers among us who tend to have home coding environments by their nature.

Regardless of the outcome of elections or leadership turn-over, change always provides opportunity. Opportunity to find the good in less than optimal situations. Opportunity to take advantage of situations and synergies that did not previously exist. Maybe even an opportunity to fix what was broken or to take proactive steps to ensure that systems and processes are more resilient in the future. An opportunity to evaluate where we are in our self-development or how we can provide assistance to others honing their craft.

In this business, things change rapidly; very rapidly. New hardware, software, and languages ensure that there is always something new to learn. This is great for the curious and those who love learning but it can be a source of frustration for others just trying to keep their heads above water. The rate at which new information is created can be overwhelming especially when people are first getting into the field. Don't lose hope. You don't need to know all there is to know about every subject. Matter of fact you can't, it's just too broad of a field to expect you'll become an expert in multiple areas. Read a little about a wide variety of topics and drill deeper into the subjects that interest you or that are required by the particular work task at hand.

The depth of this field makes it even more important to focus on what really matters; i.e. the “real” requirements. Requirements often exist in the grey area between concepts and reality and are one of the biggest sources of change I deal with on a regular basis. Requirements are broken down into tasks that dictate my day-to-day development activities. In a rapidly shifting Operational Environment, nailing down requirements can be an art form unto itself. Identifying and analyzing the “must haves” helps to narrow the scope of our development efforts and increase the amount of value-added work done each sprint.

Take inventory of what you already have, what can be reused, and what yet needs to be done with respect to the requirements that have been defined. This “delta” will result in structuring tasks in a way that minimizes the amount of new development necessary, and will increase productivity and team velocity. Doing this while anticipating what may be required down the road can help future-proof the work you are about to do or have already done. No one knows what future requirements will entail but designing software with code reuse in mind and continually growing the organization's code base with quality source code will go a long way towards decreasing the development time of future efforts.

One of the most important services the Civilian workforce can provide is continuity. Most of us are here for the long-haul and don't have to worry about being re-posted every few years. There are a lot of new faces since I first started working here and it's likely that the organization will look quite different a few years down the road. Even through numerous personnel changes, the folks who have been around awhile gain a solid understanding of where

the Unit has been and where it's capable of going. We've seen what has worked well and what actions should be avoided when possible. Each of us have a vested interest in ensuring the Unit is successful in all of its endeavors and this is especially true for everyone who plans on staying for their foreseeable future.

A sizable portion of the Civilian workforce has previous military and/or industry experience and may very well bring unique ideas and approaches to problem solving acquired during their time working with other units and organizations. This "free" resource should be embraced and frequently leveraged. Civilians are some of the best-postured to ensure the accurate and successful roll-out and implementation of long-term strategies and initiatives; stewards of change if you will. For those about to close the chapter on their Uniformed service, you should seriously consider doing what you love as a DA Civilian before heading on to other pursuits.

As Civilians, we have far fewer time constraints imposed on us compared to our Active Duty counterparts. Take advantage of this; it's another often-overlooked opportunity. This means the mission can continue to progress when Teammates are conducting other activities so don't forget to entrust and empower your Civilians to be able to carry on the fight. Let's make sure we capitalize on all of the knowledge and experience within our ranks from every available source to generate the best outcome possible. The Army can handle anything that is thrown at it so let's all do our best to embrace the inevitable changes and just get after it.

One Team. One Fight. What's your Warrior?

"SafePayload" – D Co. Developer

Disclaimer: These thoughts are my own and not endorsed by anyone that I'm aware of.

781st Military Intelligence Battalion (Cyber)

Trunk or Treat

781st Military Intelligence Battalion (Cyber)

Trunk or Treat

How Did We Get Here

By West Lewis, Senior Cyber Advisor, 782nd Military Intelligence Battalion (Cyber))

"Cyber Legion" "Silent Victory".

ON JUNE 7, 2013 THE 782ND MILITARY INTELLIGENCE (MI) BATTALION (CYBER) was activated at Fort Gordon, Georgia under the command of the 780th MI Brigade (Cyber) located at Fort Meade, Maryland. Its primary mission is to support Combatant Command (COCOM) and National Cyber requirements. Since that date the unit has evolved into one of DoD's most Elite Offensive Cyber operations unit. You may ask yourself what led to the activation of this Cyber unit.

Following the events in October 2008, where someone had managed to penetrate the military's classified network, which as we know was supposed to be fully disconnected from the public internet domain, Lt. Gen. Keith Alexander, then Director of NSA, assembled a team of trusted advisors to devise a strategy to combat future attempts to exploit or disrupt government and military network operations. During the two years leading up to the activation of the United States Cyber Command (USCYBERCOM) multiple meetings were held between government agencies and service components. U.S. Army Intelligence and Security Command (INSCOM) took the lead for building the U.S. Army Cyber forces.

The original concept was to build six 52-man detachments with locations in Georgia, Hawaii, Maryland, Texas, England, and Germany. These locations were selected based on COCOM support requirements. The detachments would be comprised of 52 civilians that would be split 85/15 to support OCO and DCO requirements (offensive and defensive cyber operations). This original concept was short lived due to the fact you need military personal to conduct Title 10 operations. In 2010, the TDA was revamped and the 2nd Cyber Battalion was born. The battalion's new structure consisted of Alpha Company, Expedition CNO; Bravo Company, Remote Operations; Charlie Company, Analysis & Production and four detachments Texas, Hawaii, Germany and England. The new TDA would allow the commander to task

organize based on requirements. Following the approval of the TDA, Ms. Lisa Bennett arrived at Fort Gordon in February 2011 as its first plank holder. She was tasked by the INSCOM commanding general to begin building the foundation that would eventually become the 782nd MI Battalion. Over the next two years Ms. Bennett would work with Fort Gordon, NSA, and INSCOM leadership to acquire operational and logistical spaces for the pending growth of the units. By the summer of 2011 the unit begin to grow. As with every plan someone always throws a wrench into it. New guidance from USCYBERCOM directed the 780th MI BDE to restructure their TDA in teams to better support directed mission. The revamped TDA structure which is still in use today and consists of the following: Battalion Headquarters, Alpha Company, Bravo Company, Charlie Company and Delta Company, all located at Fort Gordon with Echo Company located at Fort Meade, and a Detachment in Texas and Hawaii.

Following the activation of the battalion in 2013, the unit has continued to evolve to meet both service and COCOM requirements. Some of these changes have been for the betterment of the unit while others have not. Over the past five years, changes in mission's requirements have resulted in multiple changes to the work role training pipeline. Soldiers and Civilians alike can expect lifelong learning well after they complete the necessary training requirements for their work roles. As I look back over the last ten years it seem like only yesterday that we started this journey. In August of 2019 the unit reached a milestone where the number of military and civilian personnel equaled the unit identification number of 782. The battalion commander presented a Soldier with a Coin to commemorate the milestone.

Today, the 782nd MI Battalion is one of the major operating components of the Department of Defense Cyber Forces and has been recognized as a premiere Offensive Cyber force that is well trained and prepared to operate at a moment's notice. So, "What will the 782nd MI Battalion look like tomorrow?" Your guess is as good and mine. But first let's remember what got us here. Our leadership were forced to react to mission requirements with a limited understanding of the cyber environment. As we prepared for tomorrow there are several challenges that will help drive our changes. First, leaders will be better educated which should equate to a better understand of the cyber environment and better decision making. Secondly, Technology changes will influence our trainer requirements. Third, our adversaries knowledge, understand and ability to obtain new technology will also influence our decision making abilities. And lastly, mission requirements will help drive our forces structure. As we think about today we must plan for tomorrow. We will be better educated, more flexible and agile.

Leverage Change Within Us

By Genera S. Moon, Senior Analyst, A Company, 782nd Military Intelligence Battalion (Cyber)

CHANGE MEANS TO TRANSFORM or convert and in our field especially, change is inevitable. The cyber landscape is ever evolving – as is the nature with technology. The greatest catalyst for change lies within our current workforce. While we are fortunate to have some great minds and innovative thinkers, we need to do more...be more. We all have a part to play to be technologically relevant and to acclimate to the fluidity of our operating space. While each workrole has different functions and associated competencies, there is often a large disparity of available skills within the same workroles. Unfortunately, the current quantitative measurements in place do not depict the "true" health of a team, as it can be skewed by a select few. There are some that are driven to evolve with the landscape and strive for the challenge, and there will be others that will have to be held to the standard of basic competency. Which one will you be?

In every organization there are those that operate above capacity and carry a disproportionate amount of the workload, and then there are others who do not. This is not a unique phenomenon. When we apply Pareto's principle – often referred to as the 80/20 rule – to the workplace, it highlights what many of us already know; 80 percent of the work is done by 20 percent of the available workforce. Initiating change can be done

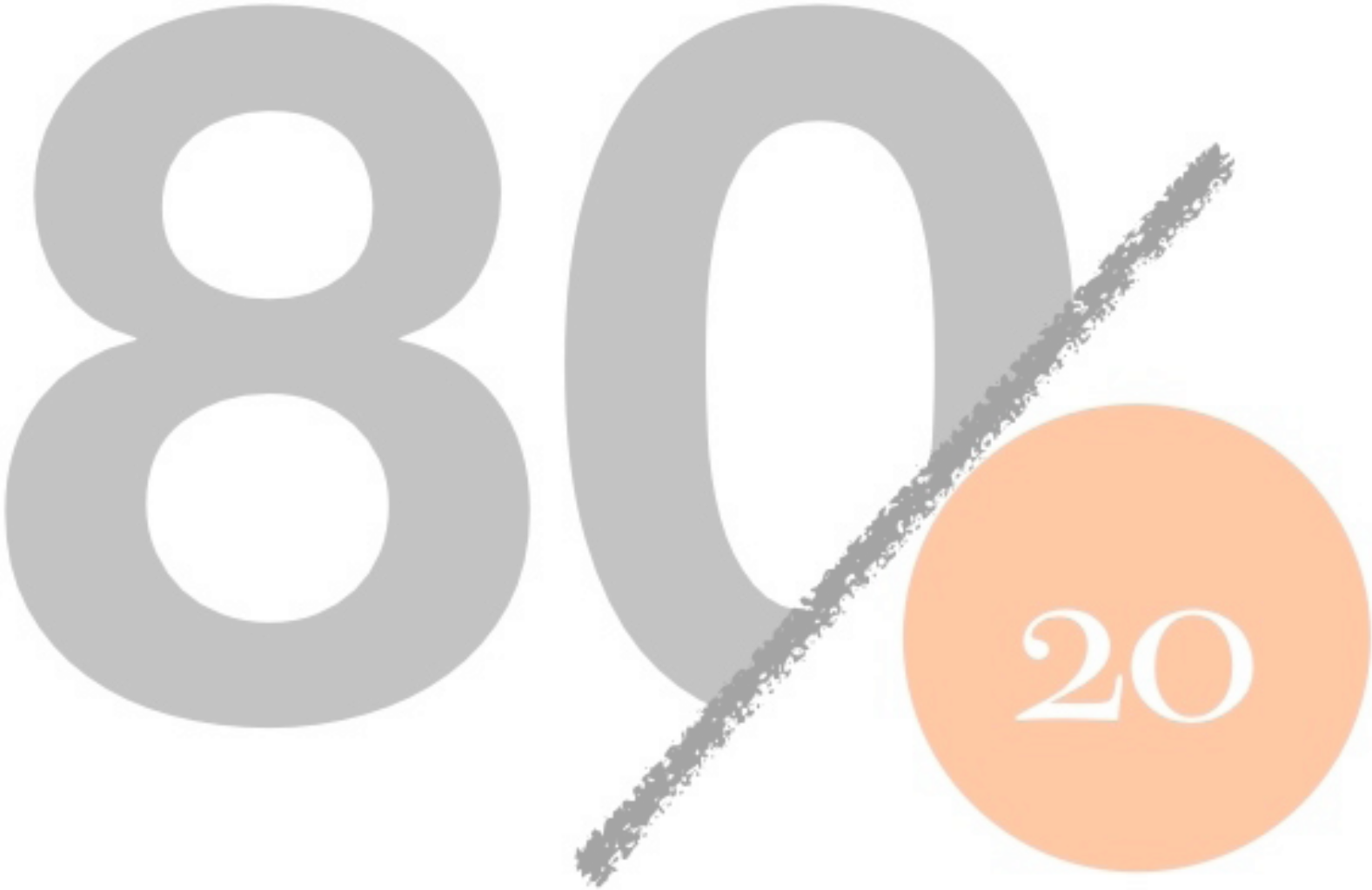


*Figure 1: P*areto's principle – often referred to as the 80/20 rule.

through addressing the disparity within workroles from two angles; improving basic competency within every workrole and implementing purposeful task management to redistribute workload.

Improving basic workrole competency

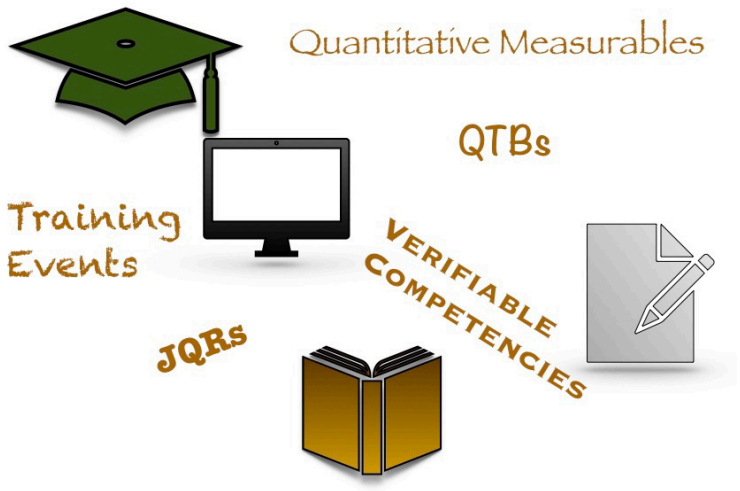


Figure 2: Improving basic workrole competency.

Some of this workrole disparity can be attributed to the team's OPTEMPO and target scope – which often dictates exposure to different problem sets and opportunity to practice our craft. That is why it is imperative that quantitative measurements like, job qualification requirements (JQRs), Quarterly Training Briefs (QTBs), training and readiness events be used better than they were intended. Through the use of established measurables, or even in some cases redefining those measurables, objective metrics establish a true litmus test that can highlight and identify where deficiencies truly lie. We need to ensure workrole standards are upheld and remain in line with a field as dynamic as Cyber and setting predetermined reassessments within the workrole would help maintain this. Verifiable competencies should be incentivized to encourage continued growth but also to reward those high performers that are driven and doing their part to professionalize in our field, whether it be through military training or civilian education.

Purposeful task management to redistribute workload

When evaluating task management through the scope of Pareto's principle, it is simply prioritizing time and resources against set tasks in a way that cultivates higher productivity. So the thought is to prioritize higher return tasks over lower return ones. In our field, the low return tasks are necessary and sometimes integral to completing the high return tasks and in no way are menial. This is where our current workforce can be leveraged in a way to be the most efficient. Align high performers to important tasks while also largely reducing the amount of low return tasks required of them; these low return tasks can be done by others. Redistribution of workload affords those that are fully qualified, driven, and already operating above capacity the opportunity to focus on higher return tasks and in turn creates a more effective organization. Managing the workforce by the 80/20 principle is the best mitigation strategy when it comes to managing workload disparity because it can reduce strain on the vital few within the workforce while holding others accountable for results.

Incentive Excellence!

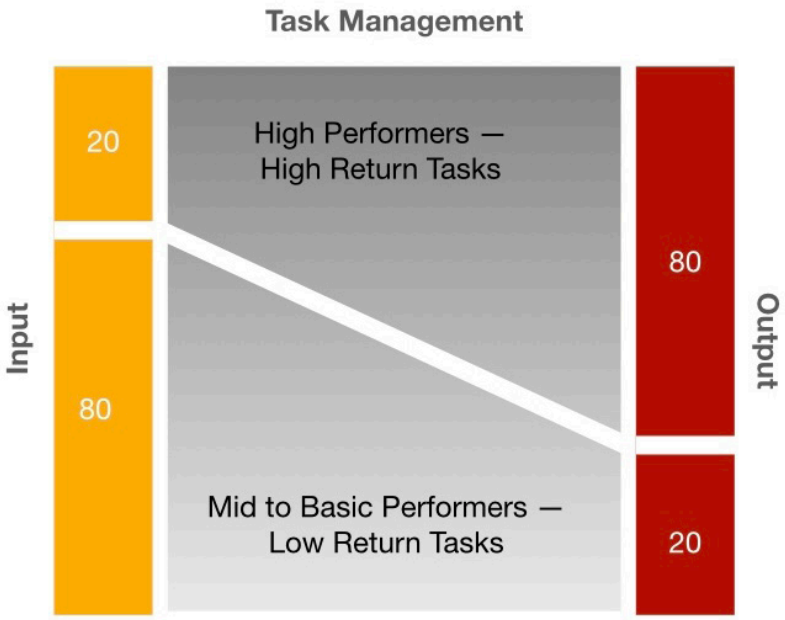


Figure 3: Purposeful task management to redistribute workload.

The Fortitude to Excel in Cyber

By Matthew D. O'Rouke, Interactive Operator, Supervisory Intelligence Specialist (Operations), B Company, 782nd Military Intelligence Battalion (Cyber)

BUILDING THE FUTURE THROUGH CHANGE is an essential task that all cyber personnel, both Soldiers and Civilians, are responsible for as both groups each have a unique contribution to the greater team effort. Soldiers will often have a wide breadth of experience and unique problem-solving approach to diverse challenges. In contrast, Civilians are highly valued for their background of expertise and in-depth institutional knowledge. These skills and perspectives combined are the strength of Army Cyber and the key to the success of the 780th Military Intelligence Brigade (Cyber). Something that Civilians get to enjoy with their longer dwell time on one station or with one unit is observing the small gradual changes over time when building out something new and exciting like Army Cyber.

Having been a part of the 780th for several years now, I have been fortunate enough to be a part of this incredible organization and see our role in the Cyber Mission Force mature as our capabilities and mission do as well. The beginning of my tour was focused on achieving Initial Operating Capability and Full Operating Capability with the Combat Mission Team structure. While this meant ensuring my capabilities met the Commander's intent, it was a necessary time to lay the groundwork for mentorship and establishing a culture of learning that would continue to impact our values for years to come. Our unit has benefited from these early actions and has produced some of the best Subject Matter Experts in cyber operations across all work roles. I passionately believe that this focus on education and expertise in Army Cyber will benefit us all for the coming change.

This focus on training and knowledge has now postured the 780th in a strategic position to support the Army's initiative as the Executive Agent for establishing both the Persistent Cyber Training Environment (PCTE) and the Joint Common Access Platform (JCAP). The PCTE platform will enable teams to simulate real-world environments to support operational mission rehearsals, validation exercises, and knowledge skills and ability (KSA) specific training scenarios to make teams and their personnel more lethal and dominant. The JCAP platform will provide the next-generation infrastructure from which teams will execute missions and operations to support future requirements as the threat landscape continues to evolve in response to national interests. The monumental tasks of developing these platforms are critical to the success not just of Army Cyber and the 780th, but for joint cyber force across United States Cyber Command. As a community of skilled experts, I am confident that we are more than up to the challenge to solidify the "information

With 780th personnel and Army Cyber Command in one location, both organizations have postured to continue to be the standard of cyber excellence and set the model for offensive cyber operations across the entirety of United States Cyber Command. The institutions we develop and the culture we establish all have a critical role in building the future of Army Cyber for the cohesive team of Soldiers and Civilians. I look forward to being a member of the 780th MI Brigade team and working with our dedicated Soldiers and Civilians in facing today's challenges to solve tomorrow's problems!

780TH MI BDE (CYBER)

782ND MI BN

CYBER LEGION
"SILENT VICTORY"

Change to Compete: A Heavily Opinionated Way to Transition from Yesterday's War and Build for Great Power Competition

By Avery Hoxworth, C Company, 782nd Military Intelligence Battalion (Cyber)

THE NATIONAL SECURITY STRATEGY OF 2017 and the National Defense Strategy of 2018 describe the present environment void of strategy – paired with global disorder and an ineffective rules-based international order. The economic agreements and international institutions established at Bretton Woods to build the post-World War II framework seem to have reached an expiration date. Their capacity to impose soft power have waned and are no longer reliable or effective stabilizers of global order. Concurrently, nefarious nation-states vying for a multi-polar world order with historic animus towards the outcome of World War II are taking advantage of this global disorder. These changes are the beginning of a complex strategic shift in our operating environment and will be accompanied by the largest national security change since the collapse of the Soviet Union. Except this strategic shift does not recognize the United States as the only hegemony.

In response to these global changes the United States' will recruit, train, and, innovate against these global competitors for the long-term future. Our organization is in the nascent phase of this strategic change, fighting last year's conflict, while transitioning to compete against global adversaries. We must take the best of our lessons learned combating terrorism nearly 20 years to provide the momentum necessary to compete against these emerging opponents. Analysts and operators highly educated against threats using throwaway systems, economical solutions, and temporary online presence will be challenged to compete against peers using complex networking devices, layered security, and government designed defense in depth methodologies. Commanders competent in Mission Command and phased warfare will instead be challenged with frequent, highly synchronize, and measured strategic objectives short of war – operations performed as part of a multi-domain effort. As the national security environment changes to compete against global adversaries so too will the cyber operating environment.

Non-linear warfare, welcome back containment. An immediate challenge among our workforce will be fighting in the early years against global competitors, while continuing to support the waning years of the Global War of Terrorism dominated currently by Phase V (Enable Civil Authority) operations. Our organization must retain their years of experience while at the same time growing their understanding of their global competitors. At some time, an inflection point is crossed and a divestment of resources and strategies from the waning fight is necessary to capitalize on the future. It is likely such an inflection point has occurred, but the speed of acceptance and transition to these new resources and strategies is delayed.

One necessary transition in strategy is a reevaluation of the "Six Phases of War" planning construct. This planning construct is the default choice against a near peer adversary, force-on-force, or high-intensity conflicts. It is linear in practice, each phase includes anticipated requirements, and provides key measurements needed to transition between phases. However, the global competitors of today compete in a non-linear manner. They are reliant upon a functioning global economy and the ability to influence outcomes within the global system. Any action performed outside of traditional Phase 0 (Shaping) operations could inadvertently degrade global integration, reducing their strategic parity. The "Six Phases of War" is not ineffective against a peer competitor, but the likelihood our organization will traverse those phases in its predictable manner is highly unlikely in our globalized economy.

This era will be dominated by peer adversaries constantly advancing among areas short of open conflict – expect the normalization of terms like irregular warfare, counter-basing operations, gray-space influence, and containment. Yes, containment is back. A clear example of this recognition is the 18 November 2020 announcement by the Secretary of Defense to elevate the U.S. Special Operations Command roughly to the same level as a separate military department. The Under Secretary of U.S. Special Operations now reports directly to the Secretary of Defense. This was done not to increase the lethality against terrorists, but instead to manage the short of conflict operations expected to occur against global competitors.

An historic example to help us move from countering terrorists to containing a peer comes from George Kennan's "X-Article" on containment of the Soviet Union. He posited a global competitor required a "long-term, patient but firm and vigilant containment" and every strategic move by a global competitor needed to incur cost and be met with a "counter-force". Other strategists of today have highlighted similar measures, calling for more than reactionary responses that are futile against peer competitors. We must compete continuously and never remain reactionary.

Full spectrum dominance, an illusion. We are no longer provided with domain overmatch and must think creatively on how to best employ our capabilities. To describe this environment the U.S. Army Training and Doctrine Command

released *Multi-Domain Battle: Evolution of Combined Arms for the 21st Century* – a doctrine reminiscent to the "X-Article". It is a method for the land domain to challenge global competitors. Instead of a linear focus on conflict, the recommendation is a continuous competition – provide no space for the adversary to operate. If an adversary denies a space, compete to turn it into contested space. These objectives impose cost, are non-linear, and support a complex operating environment.

Understanding the concept outlined in Multi-Domain Battle, Commanders need access to all domains to artfully select specific capabilities to continuously compete against the adversary. The cyber domain will be one of those many options afforded to a commander responsible for multi-domain operations. Options expected of cyber within this highly contested multi-domain environment may include us acting as the occasional strategic "counter-force", as the only domain option with the windows of opportunity to compete, or used to open a window of opportunity to enable a secondary domain to dominate. A primary planning consideration for these cyber operations will be accounting for the degraded operating environment and the lack of full spectrum capabilities or support.

An anticipated doctrine-based challenge in a Multi-Domain Battle against peer competitors is the on-going debate among experts if Mission Command remains a viable doctrine across the force. Chief of Staff of the Army Gen. Mark A. Milley described Mission Command as a form of "disciplined disobedience", but this may not be the default tool for every commander. "Disciplined disobedience" across a multi-domain environment with a Joint Force that does not use Mission Command opens vulnerabilities. The adversary only needs to force the failure of a single organization to deny our advantage. One miscalculated "disciplined disobedience" within such a highly choreographed operation is a potential disaster. As *War on the Rocks* highlighted in a 2017 article, maybe the best option is re-examining FM 100-5, the War Department's Operations manual from 1941:

The commander's decision for his unit as a whole, and the missions to subordinate units in support of the decision, are communicated to subordinates by clear and concise orders, which gives them freedom of action appropriate to their professional knowledge, to the situation, to their dependability, and to the teamplay desired.

The defining statement from the field manual is the onus placed on the commander's staff to conduct quality planning to provide clear and concise orders to subordinates. The better outputs created by the staff the increased flexibility subordinates have available to accomplish their mission. Our organization can create the built-in flexibility necessary to compete in multi-domain battles, but it requires providing the staff appropriate training to be experts in their craft and affording the time to receive and respond to missions with creative planning models Army Design Methodology.

Heavily opinionated; takeaways. Many dispersed opinions are present in this short piece. It describes a highly complex transition between grand strategies, a global disorder, and an environment where the United States is no longer afforded uncontested global freedom of movement. However, the key takeaways are relatively straightforward on how to build the future through tremendous external change: be prepared to continuously compete short of war, highly complex multi-domain battles with denied and contest space are the standard to train against, mission command should not be the default option, and an increased reliance on quality and conciseness of staff work is a must. Although some or none of these opinions based on my personal observations of world events may never come to realization, planning against future outcomes is always a productive endeavor.

Attributed References and Current Reads:

- A Whole New World (Order) – War on the Rocks Podcast
- An Answer to Aggression How to Push Back Against Beijing by Aaron L. Friedberg
- Change or Die – War on the Rocks Podcast
- Disunited Nations by Peter Zeihan
- Future warfare requires 'disciplined disobedience,' Army chief says by Todd Lopez
- Multi-Domain Battle: Evolution of Combined Arms for the 21st Century 2025-2040 by U.S. Army Training and Doctrine Command
- Multi-Domain Battle: Tonight, Tomorrow, and the Future Fight by Gen. Robert B. Brown and Gen. David G. Perks
- Origins of the Cold War The Novikov, Kennan, and Roberts 'Long Telegrams' of 1949 edited by Kenneth M. Jensen
- The National Defense Strategy of 2018
- The National Security Strategy of 2017
- To Infinity and Beyond: Battle Force 2045 – Net Assessment Podcast
- Understanding America's Declining Global Influence – Net Assessment Podcast

Mentorship Matters

By Lee W. Ries, Detachment-Texas, 782nd Military Intelligence Battalion (Cyber)

MENTORSHIP MATTERS. IT MATTERS to leaders throughout the Army and the intelligence community, throughout our command, and it should matter to you as well! The Army defines mentorship as "A voluntary and developmental relationship that exists between a person with greater experience and a person with less experience, characterized by mutual trust and respect." (AR 600-100, The Army Profession and Leadership Policy).

Mentorship matters to the Army.

Not only has the Army published guidance concerning mentorship in Army Regulations and doctrinal publications, but leaders at the highest levels extend mentorship's significance in continued efforts that will set the tone for personnel development through at least 2035. Gen. James McConville, the Army's 40th Chief of Staff, paraphrased the old adage of 'Mission First; People Always!' when he stated the Army's people strategy, *"Winning matters, and People are my number one priority."* That strategy goes on to note that "Authentic leader engagement is critical to developing cohesive teams and maximizing performance. "Although the People Strategy does not specifically highlight mentorship, FM 6-22, Leader Development, does tie mentorship to the strategy's developmental investments. By giving guidance for deliberate actions that set conditions for successful accomplishment of future objectives, Mentors advance the Army's mission and Army personnel. Mentoring has the furthest perspective of all the developmental techniques

Mentorship matters to this command.

Bringing it closer to home, our command values mentorship. Great things are happening for mentorship at every level. Col. Matthew Lennox, commander, 780th Military Intelligence (MI) Brigade (Cyber), sees mentorship as a very personal event, developed through shared experiences along with trust and respect. Senior civilian leaders across the breadth of the brigade provide mentorship to people they are helping to grow in their careers. Lt. Col. Wayne Sanders, commander, 782nd MI Battalion (Cyber), values mentorship as a key aspect of a larger personnel development effort he has begun, involving a mentorship pilot program and what is sure to become a standard across the force – the Workrole Hydra! This promises to be an invaluable tool in the kitbag of mentors throughout his battalion; ask your leadership about this new element within the 782nd.

Mentorship should matter to you as well!

Mentorship is mentee driven and mentor led. This means that its intent is to help the mentee with their goals by drawing on the mentor's experience, who helps the mentee identify and chart a path to achieving those goals. The key here is that it is not counseling or training or even coaching. Each of those is focused on personel learning and applying skills and abilities in support of the organization's goals. And if you are not sure what your goals are or should be, then you are a prime candidate for mentorship! If you do not know where to go to get connected with a mentor, take heart! There is help for you in gaining mentorship. Whether you are a uniformed Service member or Civilian, reach out to your leadership and ask. Our commanders and senior Civilians care about mentorship and can get you connected. You can also reach out to me and I will help you.

Having a mentor has made a significant impact in my civilian career. I had no idea what an Army career as a Civilian could be, aside from a string of jobs that I might apply to. My mentor helped me understand some of the programs the Army has to develop its civilian corps and the mechanisms in place to communicate intent to participate and to gain approval as well. One example of this is the Army's Enterprise Talent Management (ETM). My mentor encouraged me to apply to a program under ETM, offering guidance on the application process. I took ownership of my application process and was successful in gaining selection for the Leadership Shadowing Experience, and later the Command and General Staff Officers Course (CGSOC). Your goals may not be related to education and development, but a mentor can help you whatever your goals may be. Seek out a mentor whom you respect and who has experience you value. But if you seek a mentor who is different than yourself, you will reap benefits that come from varied perspectives.

Mentees need Mentors! Our brigade has a wealth of experience and knowledge across the command, in every career field and role that keeps the unit going and successful. If you have experience and do not have a mentee, pay close attention to those around you and identify someone who could benefit from mentorship. Seek out a mentee who is different than yourself and you will reap benefits that come from a varied perspective.

Oh, wait! Did I say that already? Yes, I did … because diversity benefits all involved: both mentee and mentor, as well as the unit and the Army!

Many may be willing to be mentors, but hesitant to take on that role. Mentorship comes from what you have gained through experience and from your own sense of responsibility and duty to the profession. Where you may feel lacking, do not despair! There is help for you to prepare to be a mentor and help for you while you mentor someone. That help can be as formal as a mentor development program or as information as a series of conversations. You can reach out to me and I will help you prepare to take on the very important role of Mentor.

Mentorship has many phases and many

faces.

Harvard's Belfer Center hosted a panel discussion on the topic of Developing Diverse Talent: A New Era of Mentorship, September 25, 2020. One of the panel members, Sandra Auchter, NGA's Deputy Associate Director for Capabilities, described her experience with mentors through the course of her career as having been varied to address different needs she faced. Early in her career, mentorship was focused on technical aspects of her job. A different mentor helped her with integration into her agency's culture. And yet another mentor helped her through continued growth through her career.

You might be in a similar place as Ms. Auchter shared. You might be new to the Civilian Corps, or new to the Army. You might be new to the cyberspace domain, or new to your location. If you are starting out fresh in some aspect of your career, you might need a mentor! One challenge I have seen, and you might have also, is that it can be hard to ask for mentorship. It can be humbling to admit that you need help in an area of your personal or professional life. If you trust that your leadership wants you to succeed, you may find it a bit easier to reach out for a lifeline. That was me, in fact! Fortunately, I now have a mentor who has been impactful to me, allowing much of the fog ahead of me to lift. Ms. Kathy Coviello, Special Advisor for Materiel Enterprise Intelligence & Security at U.S. Army Materiel Command in Huntsville, Alabama, has been my mentor since early 2018. I am fortunate along with several others to benefit from her mentorship, so she clearly takes to heart this driving concept that she expressed to me: Mentorship is an example of leadership's investment in their people.

Why write about mentorship if so much is already happening? Because there is something missing that would bring these many thoughts, concepts, actions, and efforts into a unified investment in the People who make up this brigade.

Intentionality.

Intentionality is simply being deliberate and purposeful in applying actions and investments toward an objective. We know that mentorship matters; why not be deliberate in mentorship? We cannot assume that supervisors will be the mentors that the command's personnel need. Mentorship is deeply personal. We cannot assume that personnel who want a mentor are figuring out how to get one. We cannot assume that those who have experience to share are finding mentees to share it with.

Intentionality is what we do when something matters. And mentorship matters.

In that same Belfer Center panel discussing mentorship noted earlier, Camille Steward, the Head of Security Policy for Android and Google Play, shared a simple concept of deep significance: Organizations must apply intentionality about cultivating talent. They must build systems to drive it, to cultivate it, and to incentivize it.

Driving this point home at the individual level, Col. Candice Frost, a director within the Army G-2 staff and fellow panelist in the Belfer Center event, offered this perspective on mentorship in the intelligence profession: "Mentorship must be part of the profession, expected of all and woven into the Intelligence Community's fabric to constantly reach out. Challenge yourself; apply intentionality to make change happen."

What changes do you see ahead of you for 2021? I am not talking about New Year's resolutions, but real, impactful changes. Be a Mentor. Be a Mentee. Be intentional about it and see real changes in your life, in our unit, and in our Army! ■

Army People Strategy (APS) – Civilian Implementation Plan (CIP)

By Brenda L.V. Young, Detachment-Texas, 782nd Military Intelligence Battalion (Cyber)

Issue: Data Analysis Is Not Methodical

WITH OVER 300,000 ARMY CIVILIANS, the third-largest federal employer, the Army People Strategy (APS) (2020) has a plan to ensure that their Civilians are the most ready, professional, diverse, and integrated workforce in the federal government. The Civilian Implementation Plan (CIP) is tied to and will provide changes to improve the way the Army acquires, develops, employs, and retains civilian personnel. The CIP addresses these four levels of effort that will change, enhance, and manage the Army Civilian Workforce.

Leaders in the Army identified four critical priorities to serve as a foundation for the civilian enterprise and workforce. Under the first priority, transforming workforce, planning and management, and the Army targets the proper employment of its civilian's workforce to reduce capability gaps. Leaders are working to incorporate the Defense Civilian Human Resources Management System across the force to accomplish this task.

In the past, civilian talent management has been focused on employing talent within a post or at a location. This has allowed local leaders to tailor their approach to acquire critical talent that best fits their particular needs, it also may have led to biased decisions that may not provide the best outcomes for the Army as a whole. The proposed change for our internal culture of civilian human resources management will address and prioritize results while maintaining compliance. The Army plan is to instill a new philosophy that facilitates the ability of talented Civilians – including transitioning and former service members to move into, between, and out of civilian employment opportunities in search of job satisfaction and meaningful employment. This will support a secure most talented and engaged workforce to meet our missions.

The vast majority of the civilian workforce looks to move up in their respected careers and desires a dedicated talent management and career progression process and opportunity. Proposed changes now and thruough 2028 within the Civilian Implementation Plan (CIP) should create building opportunities, changes for the future and avenues for growth for the Army Civilian Corps.

Reference:

- *https://www.army.mil/article/236347/armys_new_civilian_implementation_plan_emphasizes_talent_management*

Building the Future Through Change

By Randall G. Lewis, Analyst, Detachment-Hawaii, 782nd Military Intelligence Battalion (Cyber)

THERE HASN'T BEEN A TIME IN U.S. HISTORY when we didn't strive for building a better society. Today, we are facing a cultural change that will carry us to the future, but what are the steps to get there? It's important to objectively approach the cultural changes that are being introduced today. Cyberspace is a domain that is constantly evolving and changing, but we show no fear in the face of those changes. We can look to the armed forces' approach to change in the past to shape our future in cyberspace.

The global health crisis caused by the Coronavirus Disease 2019 (COVID-19) redesigned our way of life with new social reforms. We depend on each other more than we used to for our own safety. Throughout history we have depended on members of society to build together. How can we reorient our dependencies to build for the future in cyberspace?

In May 2011, former President Barack Obama's International Strategy for Cyberspace started with: "Prosperity, Security, and Openness in a Networked World" for "Building on Success" (1). He focused on businesses and communities for the future of a growing world. The key word being "communities" as the foundation starts and ends with us, our greatest asset. What will our workforce look like in 10 years with 50 percent of all Americans under age fifteen identifying as a Black or Latino?

Similar to our social challenges in 1948, former President Truman signed exec order 9981, which abolished segregation in the armed forces. By looking to the examples of the past as well as the future, we allow ourselves to unify our great forces to what we are today. Truman stated after signing "There shall be equality of treatment and opportunity for all persons in the armed forces without regard to race, color, religion or national origin."

A document alone does not make change, we need action and social change. We can get there by inclusively hiring and recruiting. Also by mentoring and reaching out to communities that would not have access and changing our mindsets of who we thought were the best candidates.

The U.S. Army Air Corps (1926 – 1941) was initially looked at as an auxiliary support for ground forces by traditionalists instead of as a separate and equally important force. That would eventually form the U.S. Army Air Forces (1941) before leaving the Army in 1947 and forming the mighty Air Force, post-WW2.

Culturally our society is going through a huge shift. Change has been chanted, marched to, and sacrificed for. With a large portion of our citizens united for change, there will be those that want things to stay the same. While cultural and social laws are what moves a society, legal laws stabilize us. In a stand for equality, where will we be as an organization to usher in new Cyber Warriors?

General Shinseki who was the 34th Chief of Staff of the Army along with the first Asian-American Four Star general and Secretary of Veterans Affairs. He looked towards the future when he transformed heavy and light brigades into a medium-weight structure that would allow them to be air deployed anywhere in the world, against traditional ideas. He stated: "If you don't like change, you are going to like irrelevance even less."

The U.S. Cyber Command (2) started in 1972, where "consultants for the DoD warned of serious vulnerabilities" and "the importance of cyberspace to national security". In time, certain points in Cyber Command history took place:

- Dec. 1, 1998 , JTF-CND attained initial operating capability
- Jan 2000 Joint Task Force – Computer Network Operations (JTF-CNO)
- 2004, JTF-CNO evolved into Joint Task Force - Global Network Operations (JTF-GNO),
- Cyberspace was declared a domain, alongside air, land, sea and space
- 2005, Joint Functional Component Command for Network Warfare (JFCC-NW) was established
- June 23, 2009 , U.S. Cyber Command (USCYBERCOM) established

Cyber command went through changes to get to where we are today. General Paul M. Nakasone, the commander of U.S. Cyber Command and director, National Security Agency/Chief and Central Security Service stated "we have learned that capabilities rapidly change; accesses are tenuous; and tools, techniques, and tradecraft must evolve to keep pace with our adversaries."(3)

Our adversaries are watching our every move. From our presidential debates to protest, welfare to healthcare, economic bust to boom. We have built from ground up, with a united front. Our future is us, our agencies, people, country and citizens.

References:

- *https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf*
- *https://www.cybercom.mil/About/History/*
- NDU, Press. (2018). An Interview with Paul M. Nakasone. Retrieved 2020, from *https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-92/jfq-92_4-9_Nakasone-Interview.pdf*

Senior Civilian Advisor Role

By Selina Desler, Detachment-Hawaii, 782nd Military Intelligence Battalion (Cyber)

PRESIDENT BARACK OBAMA emphasized, "We cannot continue to rely only on our military in order to achieve the national security objectives that we've set. We've got to have a civilian national security force that's just as powerful, just as strong, just as well-funded." While several agencies recognize the importance of senior civilian advisors (SCA) roles in mission-continuity, SCAs within Cyber still face several challenges with being recognized as equals to their military counterparts. In order to build the symbiotic relationship of mutualism which enables SCAs to perform to the level in which they were hired, they must first be treated in the same stature of that position. Additionally, with continuous permanent change of station (PCS) among military personnel, mission continuity is heavily relied upon by civilians who do not always have an equal voice within that mission set. Enabling SCAs to perform functions ordinarily conducted my military personnel in terms of evaluations, mission leadership, and decision-making will build the powerful civilian workforce.

The National Security Agency (NSA) learned that in order to preserve mission continuity, a strong civilian workforce was needed to maintain those missions. The NSA concept still maintained military leaders as the overall hierarchy, but among its organizations, positions directly affecting the outcome of the mission; such as Division Leader, Branch Lead, and Section Lead, were predominantly held by civilian personnel in order to build the subject matter expertise needed to advance the mission. While military personnel play a significant role within the mission in terms of providing leadership to other service members as well as technical expertise, the NSA understood their time within the mission would be temporary. The Cyber concept placed military members in the roles that directly affect mission, with senior civilians working as advisors to military personnel. The NSA construct is not better than the Cyber construct, but the Cyber construct can only work if there is a symbiotic relationship between the senior military leadership (SML) and the SCA. In order for this relationship to work, the SCA must be viewed as an equal to its military counterpart; this concept must include complete transparency between both individuals. An example of the lack of transparency between an SML and SCA in which I witnessed resulted in the loss of information that was needed in order for the SCA to do their job properly. Although isolated incidences happen, when it becomes habitual for SMLs do not include SCAs in important meetings or discussions, or allow them to make decisions affecting mission outcome as well as health and morale of the staff, and SCA is no longer working with the SML, but trying to survive them instead. This type of behavior can create work environments no longer conducive to productivity. The aforementioned incident, as well as others could be avoided if emphasis is placed on the fact the SCA and SML are equals and share the duties and responsibilities of the mission together; one serving as the continuity to progress the mission and the voice of reason, and the other to provide new and fresh ideas from the military stance, and who is not afraid to take risks.

PCSs are another issue in the role of SCAs. Although it is not uncommon for civilians to relocate jobs, SCAs are more likely to stay in a position much longer than their military counterparts. With Cyber still in a growing stage, the military personnel needed in order to maintain a mission is at minimal manning in most cases; in this same regard, the civilian population is not extensive either. What an SCA offers to a mission is the continuity needed in order for the mission to continue. An SCA brings a world of experience that can sometimes be ignored by some SMLs because they do not wear a uniform; this is not prevalent among all SMLs, but it does occur. When a situation arises in which an SML is new or does not have the expertise on a particular topic, the subject matter expert, who is usually a civilian, is relied on to make a sound decision that is both beneficial to the mission and the overall health of the environment; this is how it should work, and in most cases, it does work in that manner. However, there are situations in which an SML ignores their SCA simply because they want to be the final decision maker on the matter, even if they are not the most knowledgeable person on the matter. When this occurs, decisions are made that can impact not only the mission, but the health and morale of every mission member.

Most SCAs at one point or another wore a uniform, they understand the military construct and the pressure to not only be an exemplary service member, but also a contributing member of a team. Our military is given a lot of responsibility and there are not enough hours in the day for them to accomplish all the tasks they are assigned. Allowing SCAs to rate military personnel can ease some of the pressure placed on the SMLs. If Army O3 is allowed to rate a GG14, why can GG14 not write an OER for the Army O3? In that same manner, if an SCA is placed in a supervisory role, why would the supervisory role not encompass the military that are also there? This would allow SCAs to properly mentor and shape the workforce according to mission needs while working with SMLs to create a cohesive environment.

In all, the SCAs are the SMLs greatest advocates, and in most cases, the relationship between the two is phenomenal with mutual respect given by each in their perspective roles. The risk of losing an SCA from a mission comes when it is a one-sided relationship, and there are plenty of instances of those as well. Creating an equal partnership between the two will truly exemplify the "one team, one fight" concept. ■

782nd Military Intelligence Battalion (Cyber)

Trunk or Treat

FORT GORDON, Ga. -- The command team and Family Readiness Group volunteers from C Company (Centurions), 782nd Military Intelligence Battalion (Cyber), participated in the garrison Trunk or Treat., October 30.

FORT GORDON, Ga. -- Kismet Hennessy, Capt. TJ Hennessy's dog dressed up for Halloween.

FORT GORDON, Ga. -- Kearby Chess dressed up, as authentically as possible, as Indiana Jones for Halloween

782nd Military Intelligence Battalion (Cyber)

Christmas House

FORT GORDON, Ga. -- The command team from C Company (Centurions), 782nd Military Intelligence Battalion (Cyber), delivers toy donations on behalf of organization to the Fort Gordon Christmas House, December 3.

.

FORT GORDON, Ga. – A Company (Archers), 782nd Military Intelligence Battalion (Cyber), delivered over 500 toys to the Fort Gordon Christmas House along with the other tenet units on the installation. The Archers were able to secure a new streamer as a result of winning the competition for the most toys donated, pictured left to right are Pvt. Cierra Shakir, Sgt. 1st Class Thomas Ryan, Capt. TJ Hennessy, Staff Sgt. Kenneth Owens, and Sgt. Yohan German.

The Army's Only Cyber Warfare Battalion Confirms Training Program

By Steve Stover, Public Affairs Officer, 780th Military Intelligence Brigade (Cyber)

BUTLERVILLE, IND. – SOLDIERS from the 915th Cyber Warfare Battalion, headquartered at Fort Gordon, Georgia, conducted a Field Training Exercise at Muscatatuck Urban Training Center, October 1 through 12, to provide a dedicated training environment for the Army's first Expeditionary CEMA Team, ECT-01, and refine cyber gunnery tables for future certification exercises.

According to U.S. Army Cyber Command, the 915th CWB is the first scalable organic expeditionary capability to meet the Army's current and projected tactical Cyberspace Electromagnetic Activities (CEMA) requirements. The battalion, through its Expeditionary CEMA Teams (ECTs) provides a scalable capability to deploy cyberspace operators to conduct operations to deny, degrade, disrupt, destroy and manipulate cyberspace and electromagnetic effects for Army maneuver commanders.

Lt. Col. Matthew Davis, commander, 915th CWB, said the purpose of the FTX was two-fold.

"Priority one is the ECT's training proficiency and having a scenario constructed around them as a training audience." said Davis. "The second purpose is to develop a training plan for how we are going to train ECTs as we build them. This is our first ECT and there are 11 more to come – so how are we going to train them. We have a draft, a beta, and this is a pilot run of the beta to figure out have we established the right task, condition, and standards, training objectives, and is this the right training plan."

According to Jim Greig, 780th Military Intelligence Brigade (Cyber), S3 Plans, "Of all the training areas available in the Department of Defense, MUTC is the most realistic, complete, robust and appropriate facility."

MUTC is a 1,000-acre urban training facility near Butlerville, Indiana, with over 200 buildings, to include a multi-story hospital, fresh-water and waste-water treatment facilities, a coal-fired steam plant, an embassy, high school, and even a prison – and "everything here is linked and in play," said Greig.

"At the National Training Center, the RTU (rotational training unit) is the training priority. Here, we are the training audience," added Chief Warrant Officer 2 Jacob Hogue, the battalion's operations technical advisor. "The ECT is running through their processes and refining their TTPs (tactics, techniques and procedures). It's also giving the battalion an opportunity to really figure out what we need to have for (cyber) gunnery tables. It gives us the opportunity to refine our training program."

Maj. Richard Byrne, a cyberspace operations officer and team leader for ECT-01, said the MUTC FTX provided his Soldiers an opportunity to train on both technical and tactical tasks for the team and gave the ECT-01 plans section the ability to exercise command and control of staffing processes and coordinating effects.

The ECT-01 plans section discussed the staffing process and the benefits of MUTC not only for the 915 CWB, but for the Army.

"We tailor our CONOPS (concept of operations) to the (maneuver) commander's intent, we take his intent for that mission and derive an effect from that," said Staff Sgt. Robert Vickery, a fire support specialist (13F) in the ECT-01 plans section.

"Intel drives the fight," said Staff Sgt. Austin Moss, a fire support specialist (13F) in the ECT-01 plans section. "So, we task a team to look for something in a specific area, and from that gathered information it will go through a process, a kind of 'what is there process,' and then based on what is there, the commander will make another decision based on it."

"This is the first time I have seen an exercise like this in cyber where we are able to go out and link a bunch of pieces together," added 1st Lt. Courtney Sullivan, a cyberspace operations officer (17A) in the ECT-01 plans section. "Where we're able to come and have actual OPORDs (operations orders) that are directed towards a cyber mission and tasks our ECTs to test their capabilities and equipment, test their ability to operate that equipment, and really gain that confidence in themselves and how they function with each other and their equipment."

"We're building SOPs (standard operating procedures) and identifying how we execute things efficiently because that hasn't been done before," said Vickery. "That's one big takeaway. Another thing MUTC provides is a realistic urban environment where you can actually see effects. When you go to NTC or JRTC (Joint Readiness Training Center), most of the time effects are white-carded, these guys are actually getting to see the results."

Byrne summarized the capabilities ECTs will provide for maneuver commanders now and into the future at the Corps echelon and below.

"Our job is to support the Corps tactical fight," said Byrne. "We're here to employ cyber and electromagnetic activities for that commander, integrate with his staff, and provide him with a tactical edge over his adversaries."

With 11 more ECTs being formed to support the U.S. Army's multi-domain operations, Command Sgt. Maj. Marlene Harshman, the battalion's senior enlisted leader, said the lessons learned from FTX have been "priceless."

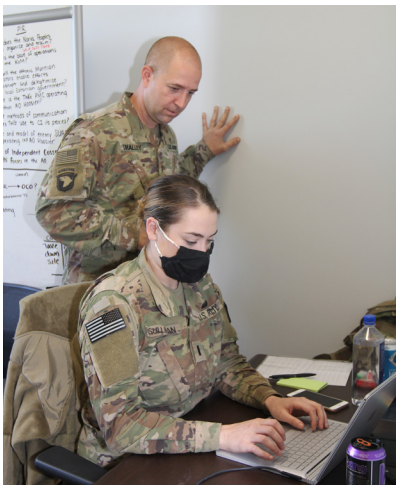
"The lessons learned from the FTX will build on our current and future capacity. We have to constantly focus on the future

and adapt to make expeditionary cyber better, with every operation and every lesson learned," said Harshman. "MUTC provided that dynamic environment for us to learn and grow as a team. That was critical in this first-ever event where the entire ECT was exercised. The lessons learned have been priceless."

BUTLERVILLE, Ind. *– 2nd Lt. Anthony Walton, a cyberspace operations officer assigned to the battalion S-3 (operations) section, 915th Cyber Warfare Battalion, briefs the 780th Military Intelligence Brigade (Cyber) leadership on the battalion's Field Training Exercise at Muscatatuck Urban Training Center, Oct. 7.*

BUTLERVILLE, Ind. *– Maj. Richard Byrne, a cyberspace operations officer assigned to the 915th Cyber Warfare Battalion, is the team leader for Expeditionary CEMA (cyberspace electromagnetic activities) Team, ECT-01, and is participating in the battalion's Field Training Exercise at Muscatatuck Urban Training Center, Oct. 7.*

BUTLERVILLE, Ind. *– Staff Sgt. Austin Moss, a fire support specialist (foreground), and Sgt. 1st Class Brian Samuels, Expeditionary CEMA (cyberspace electromagnetic activities) Team, ECT-01 plans section NCOs, are participating in the battalion's Field Training Exercise at Muscatatuck Urban Training Center, Oct. 7.*



BUTLERVILLE, Ind. *– 1st Lt. Courtney Sullivan (sitting), a cyberspace operations officer, and Chief Warrant Officer 2 Philip Smalley, an electronic warfare technician, Expeditionary CEMA (cyberspace electromagnetic activities) Team, ECT-01 plans section, are participating in the battalion's Field Training Exercise at Muscatatuck Urban Training Center, Oct. 7.*

Adaptability of the 915th

By 2nd Lt. Patrick M. Paris, Cyberspace Capability Developer, 915th Cyber Warfare Battalion

This article is an overview of the mission of the Army's first scalable organic expeditionary cyber battalion -- the 915th Cyberspace Warfare Battalion -- and how the unit accomplishes that mission while adapting to meet Army requirements."
Mission: "The 915th Cyberspace Warfare Battalion conducts information warfare in support of Army requirements."

THE WHO – "THE 915TH CYBERSPACE WARFARE BATTALION…"

Although the U.S. Army activated the 915th CWB in May 2019, the history of the battalion's formation began almost six years ago. The origins of battalion date back to 2015, when ARCYBER's CEMA (Cyberspace Electromagnetic Activities) Support to Corps and Below (CSCB) pilot program began helping to shape the Army's ability to fully integrate cyberspace, electronic warfare, information operations and tactical signals intelligence operations with fires and protection at the Army corps level and below in support of Multi-Domain Operations (MDO).

Since then, the 915th has taken part in major training exercises at the Army's Combat Training Centers at Fort Irwin, Calif.; the Joint Readiness Training Center at Fort Polk, La.; and the Joint Multinational Readiness Center in Hohenfels, Germany, as well as with Army Special Operations Forces such as the 75th Ranger Regiment. The battalion's operations include Defensive Cyber Operations in support of network infrastructure, Offensive Cyber Operations to degrade enemy command and control capabilities, as well as Cyber Intelligence,

Surveillance and Reconnaissance missions to support employment of CEMA effects at the tactical level. These pioneering operations help to guide and shape the cutting edge nature of the 915th and its ability to adapt to the needs of the Army.

The "WHAT" – "…conducts information warfare…"

The Army uses these exercises and real-world events to develop organization, equipment and mission capabilities in support of Army force modernization and MDO, and help ensure the battalion is equipped with the mechanisms and methods to function in extreme environments and face the challenges of ever-changing technologies that modern tactical forces will likely encounter in combat. The 915th's efforts have helped the Army to develop a better understanding of how to employ cyber forces in tactical settings, and a new focus on maneuver in the information environment as an integral component of modern tactical combat.

The structure of the 915th allows it to provide manned, trained and equipped Expeditionary Cyber Electromagnetic Activities Teams (ECTs) to support maneuver unit commanders and exploit cutting-edge technology across all five warfighting domains to attack, defend and influence objectives in the information environment.

The "WHY" – "…in support of Army requirements."

As the 915th grows, it will activate and manage multiple ECTs to support deployed units engaged in MDO. Which leads to the "why".

"The Army is in a transition in a lot of ways, but one of the most important is transitioning from COIN [counter-insurgency operations] to LSGCO [large scale ground combat operations] and MDO," said Lt. Col. Matthew Davis, commander of the 915th. "The 915th CWB will need to adapt to these larger changes to fit within those domains."

In recent years the Army has primarily been at war with smaller insurgencies in Iraq and Afghanistan. These insurgencies are widespread and use subterfuge and technology to augment their limited size against the much larger U.S. force. But in LSGCO and MDO the U.S. may face a much different fight against peer or near-peer adversaries. To help ensure it can decisively fight and win against such opponents, the Army is also leveraging innovation throughout the force.

Technology has become critical to our success, which is why the 915th exists. For example, when a U.S. Army infantry patrol conducts a raid, the ability to reduce its electromagnetic signature to avoid enemy detection, exploit the objective for technical data, and locate adversaries based on their electromagnetic signature, help to assure their success and survival.

The 915th is constantly adapting and developing to meet the Army's information warfare requirements. One good example: the battalion recently deployed an ECT to the "Cybertropolis" of the Indiana National Guard's Muscatatuck Urban Training Center to refine its cyber gunnery tables for future ECTs.

The 915th is preparing to scale for the battlefields of the future, continually leveraging innovation and modernization in support of Army requirements. ■

BUTLERVILLE, Ind. – Army Specialists Mike Diep (left), and Matthew Scruggs, 17C, are members of an Expeditionary CEMA (cyberspace electromagnetic activities) Crew, ECT-01, assigned to the 915th Cyber Warfare Battalion, participated in a Field Training Exercise at Muscatatuck Urban Training, October 1 through 12.

BUTLERVILLE, Ind. – Soldiers from the 915th Cyber Warfare Battalion, headquartered at Fort Gordon, Georgia, conducted a Field Training Exercise at Muscatatuck Urban Training Center in order to assess and refine cyber gunnery tables for future certification exercises, October 1 through 12.

BUTLERVILLE, Ind. – Capt. Richard Shmel, a 17A, cyberspace operations officer, who hails from Eden Prairie, Minn., participated in the 915th Cyber Warfare Battalion's Field Training Exercise at Muscatatuck Urban Training, October 1 through 12.

BUTLERVILLE, Ind. – Pfc. Dylan Taylor, a 17C, cyberspace operations specialist, who hails from Long Beach, Calif., is participating in the 915th Cyber Warfare Battalion's Field Training Exercise at Muscatatuck Urban Training, October 1 through 12.

BUTLERVILLE, Ind. – Lt. Col. Matthew Davis, commander of the 915th Cyber Warfare Battalion, and Command Sgt, Maj. Marlene Harshman, the battalion's senior enlisted leader, conducted an after action review (AAR) during the battalion's Field Training Exercise at Muscatatuck Urban Training Center, October 8.

Hunt Forward Estonia: Estonia, US strengthen partnership in Cyber Domain with Joint Operation

FORT GEORGE G. MEADE, M.D. — ESTONIAN AND U.S. cyber commands jointly conducted a defensive cyber-operation on Estonian Defence Forces' networks from September 23 to November 6. The operation, designed to counter malicious cyber actors, strengthened the cyber defense capability of both nation's critical assets.

"Combined operations with our closest allies like U.S. are vital for ensuring security of our services. These kind of operations provide our operators an opportunity to exchange best practices as well as give us objective feedback on our current defense posture in cyber domain. This operation is another successful milestone in our cooperation with U.S. partners," said Mihkel Tikk, Deputy Commander of Estonian Defense Forces Cyber Command.

Working together, cyber specialists from the U.S., referred to as "Hunt Forward" teams, and Estonian cyber personnel from Defense Forces Cyber Command, hunted for malicious cyber actors on critical networks and platforms. The U.S. had previously partnered with various countries throughout Europe, however, this defensive cyber operation marked the first of its kind between the U.S. and Estonia.

"Despite the challenges of a global pandemic, we safely deployed to Estonia, and other European countries, for several weeks to gain unique insight into our adversaries' activities that may impact the U.S.," said U.S. Army Brig. Gen. Joe Hartman, Commander, Cyber National Mission Force. "Our teams proactively hunt, identify and mitigate adversary malware and indicators. We then share that malware broadly, not just with the U.S. government but with private cybersecurity industry and allies, which directly increases the overall security of U.S. critical infrastructure and related networks."

For the U.S., Hunt Forward teams play a crucial role in U.S. Cyber Command's "persistent engagement", an effort aimed at countering malicious cyber activity below the level of warfare. USCYBERCOM personnel are specially trained to secure and defend government networks and platforms against adversaries. The U.S. military's Defend Forward strategy leverages key partnerships to address malicious cyber activity that could be used against U.S. critical infrastructure.

"Estonia is a digital society and we depend on cyber everywhere, as well as in defense. For us it´s really important to be one of the first Allies with whom the US has initiated this kind of joint operation, which enabled us to obtain an independent assessment on our networks. As a leader in cyber, it also provided Estonia an opportunity to share best practices to better protect our networks," said Margus Matt, Undersecretary responsible for cyber defense at the Ministry of Defense of Estonia.

Both nations benefit from such partnerships as it provides an opportunity to improve cyber defense by assessing potential threats, while also contributing to global cybersecurity. Disclosing malware enables greater protections for users both in public and private sectors around the world.

"Cyber is a team sport – when it comes to halting threats from cyberspace, no one can go it alone," said Thomas Wingfield, Deputy Assistant Secretary of Defense for Cyber Policy. "Our strategy hinges on collaborating with our allies and partners, with the private sector and academia, and with state and local governments to ensure cyberspace remains a safe, secure, and open engine of innovation and prosperity." U.S. Cyber Command, in cooperation with U.S. European Command and NATO allies, continuously work to deter malicious cyber activity in the region.

The two countries have ongoing cooperation at various levels within USCYBERCOM, U.S. European Command, Maryland National Guard, and Sixteenth Air Force (U.S. Air Forces Cyber).

"U.S European Command's robust Cyber Security Cooperation program is focused on building Allied and partner cyberspace operational capabilities, which strengthens trust and cultivates strong ties with our cyber partners throughout Europe. Through bilateral and regional security cooperation efforts and information sharing initiatives, we are able to further enhance our collective cybersecurity posture as well as enable Hunt Forward operations in our area of responsibility," said U.S. Army Brig. Gen. Maria Biank, director of USEUCOM's C4 and cyberspace directorate.

The main mission of the Estonian Cyber Command is to provide command support to the governance area of the Estonian Ministry of Defense. The establishment of the Command in 2018 has been part of the efforts to strengthen Estonian cyber defense posture and thereby contribute to ensuring the security of Estonia in general.

780TH MI BDE (CYBER)

"EVERYWHERE AND ALWAYS...

...IN THE FIGHT!"

781ST MI BN
"VANGUARD"

PRAETORIANS

782ND MI BN
"CYBER LEGION"

915TH CWB
"HARBINGER"

HHC, 780TH MI BDE
"HASTATI"

PRAETORIANS
"STRENGTH AND HONOR"

FORT GEORGE G. MEADE, Md. – Chief Warrant Officer 4 (CW4) Erin Ward was promoted to CW4 by Col. Matthew Lennox, commander of the 780th Military Intelligence Brigade (Cyber), in a ceremony in front of her fellow Soldiers, Family, and friends on the soccer field next to the Brigade headquarters, Dec. 2.

WASHINGTON, D.C. – Soldiers and Army Civilians from the 780th Military Intelligence Brigade (Cyber) visited the Museum of the Bible to "learn about the history of the Bible and its impact around the world," in an event hosted by the Brigade Unit Ministry Team on October 30.

FORT GEORGE G. MEADE, Md. – Chaplain (Maj.) Kevin White, brigade chaplain for the 704th Military Intelligence (MI) Brigade, who previously served as the chaplain for the 782nd MI Battalion (Cyber), was the guest speaker at the 780th MI Brigade quarterly fellowship luncheon in the brigade annex, Oct. 21. Chap. White spoke about "connections" – our connections to God and each other – and in his sermon quoted Mathew 6:6 and Ecclesiastes 9:4-12..

FORT GORDON, Ga. -- A Company (Archers), 782nd Military Intelligence Battalion (Cyber), held an NCO promotion ceremony for five new up and coming NCOs on Nov. 6. Standing in the front, from left to right: Sgt. Noah Chestnut, Sgt. Tyson Freeman, Sgt. Yohan German, Sgt. Steffan Hinkle, and Sgt. Nicholas Nguyen..

FORT GEORGE G. MEADE, Md. -- Specialist Adam Alim is the BOSS (Better Opportunities for Single Soldiers) representative for the 781st Military Intelligence Battalion (Cyber). Alim is a highly motivated and dedicated Soldier who inspires to make change in his unit and community. With an enormous amount of enthusiasm, energy, and support, Alim is determined to successfully fulfill his role as the Battalion BOSS Representative!

FORT GEORGE G. MEADE, Md – Lt. Col. Chan Yang Shin, E Company, 782nd Military Intelligence (MI) Battalion (Cyber), was promoted to lieutenant colonel by Col. Matthew Lennox, commander of the 780th MI Brigade (Cyber), in a ceremony in front of his fellow Soldiers, Family, and friends on the soccer field next to the Brigade headquarters, Dec. 11.

When Tragedy Strikes Us Hard We Need Hope

By Chaplain (Capt.) John K. Han, 781st Military Intelligence Battalion (Cyber)

I REMEMBER WATCHING A DOCUMENTARY CALLED, "THE ULTIMATE KILLING MACHINES." The documentary analyzed the tactics of a predator and prey. It showed how the prey was vulnerable and oblivious to its surrounding environment. It kind of reminds me of a harmless sheep in the middle of a dark forest, surrounded by ravenous wolves. The sheep is clueless to what danger lurks around the corner of a dark forest.

Our lives are very much like that of a helpless and harmless sheep. We are living in a world that is filled with all kinds of tragedies ready to strike us at any given time and we are vulnerable. The Predator is Tragedy and the Prey is us. Tragedy strikes us hard when we least expect it. As Soldiers and Family members, we most likely experienced more than one tragedy in our lives. Tragedies can include, i.e., the loss of our loved one(s), toxic relationships, financial crisis, spiritual warfare, and the list goes on and on and on; with everyone experiencing some type of tragedy that is unique, but similar in nature.

What tragedies have you experienced in your life? What tragedy is weighing you down at this moment that you feel like there's no Hope? Well, let me tell you something wonderful; God gives us hope through His Divine Word. Whenever I think of a tragedy in the middle of the valley of the shadow of death, I think of a Scripture passage found in the book of Psalm.

Psalm 23 offers us hope:
"The LORD is my shepherd; I shall not want. He makes me to lie down in green pastures; He leads me beside the still waters. He restores my soul; He leads me in the paths of righteousness For His name's sake. Yea, though I walk through the valley of the shadow of death, I will fear no evil; For You are with me; Your rod and Your staff, they comfort me."

As a vulnerable and helpless sheep, I look to the one and only Shepherd Jesus Christ for comfort, even when I am faced with tragedies in my life. I know that the good LORD will stand beside me and never leave me nor forsake me. Although my families and friends leave me; He will never forsake me, now that's Hope. I know deep inside that the good Shepherd got my six when I need him the most and He will also give you the strength, Hope, and resilience if you simply trust Him.

I conclude this article with this poem, "Footprints in the Sand."

"One night I dreamed I was walking along the beach with the Lord.
Many scenes from my life flashed across the sky.
In each scene I noticed footprints in the sand.
Sometimes there were two sets of footprints,
other times there were one set of footprints.
This bothered me because I noticed
that during the low periods of my life,
when I was suffering from anguish,
sorrow or defeat,
I could see only one set of footprints.
So I said to the Lord,
"You promised me Lord,
that if I followed you,
you would walk with me always.
But I have noticed that during
the most trying periods of my life
there have only been one
set of footprints in the sand.
Why, when I needed you most,
you have not been there for me?"
The Lord replied,
"The times when you have
seen only one set of footprints,
is when I carried you.""

-Mary Stevenson

ARMY CIVILIAN CORP CREED

I AM AN ARMY CIVILIAN – A MEMBER OF THE ARMY TEAM.

I AM DEDICATED TO OUR ARMY, SOLDIERS AND CIVILIANS.

I WILL ALWAYS SUPPORT THE MISSION.

I PROVIDE LEADERSHIP, STABILITY, AND CONTINUITY DURING WAR AND PEACE.

I SUPPORT AND DEFEND THE CONSTITUTION OF THE UNITED STATES AND CONSIDER IT AN HONOR TO SERVE OUR NATION AND OUR ARMY.

I LIVE THE ARMY VALUES OF LOYALTY, DUTY, RESPECT, SELFLESS SERVICE, HONOR, INTEGRITY, AND PERSONAL COURAGE.

I AM AN ARMY CIVILIAN.

780TH MILITARY INTELLIGENCE BRIGADE

NEXT QUARTER'S BYTE IS focused on "**AvengerCon 5**". If you presented at the conference or if you have a white paper worth sharing across the information warfare enterprise, write a synopsis paragraph and send it to Steven Stover at steven.p.stover.civ@mail.mil NLT Feb. 1, 2021. Articles are due NLT Mar. 1, 2021.