780th MILITARY INTELLIGENCE BRIGADE (CYBER)

THE BYTE

Vol. 10, Issue 1

780th MI BRIGADE TENTH ANNIVERSARY

December 1, 2011 - December 1, 2021

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

780th MI Brigade Tenth Anniversary

In this issue of the BYTE magazine, the Praetorian Soldiers, Civilians, past and present, celebrate the 780th Military Intelligence Brigade's tenth anniversary. The 780th MI BDE officially unfurled its colors for the first time during a ceremony at Fort Meade, Maryland on December 1, 2011, and ever since, the brigade's mission has increased in scope, scale, and complexity. The unit is known among U.S. Army Cyber Command, U.S. Cyber Command, and senior Army leaders as a world class cyberspace operations force capable of providing a ready force, developing capabilities required to meet expanding requirements, and delivering effects at the time and place of the operational commander's choosing.

Although the focus of the magazine is on the Brigade's anniversary, the Soldiers and Civilians of the 780th MI BDE: HHC/780 MI BDE (Hastati); 781st MI Battalion (Vanguard); 782d MI BN (Cyber Legion); 915 Cyber Warfare BN (Leviathans); and Task Force Echo – past and present, as well as those who preceded the brigade's activation, have each had a significant part in contributing to the organization's history and success.

"Everywhere and Always…In the Fight!"

Steve Stover
Public Affairs Officer, 780th MI BDE
Editor, The BYTE

Praetorian 6: Happy Anniversary!

PRAETORIANS,

The Command Sergeant Major and I are proud to lead this incredible organization and thrilled to see it continue to grow and mature.Having been around the brigade for six of the last seven years, I find it awesome to see the brigade continue to be the workhorse for U.S. Cyber Command. There has been growth in manning, mission, and capability. The brigade now consists of four battalions: 781st, 782d, 915th, and Task Force Echo (TFE). More impressive is the growth in mission. Every mission team has a relevant target and makes progress consistently. I laugh now at how hard we worked on 61 National Mission Team to get people trained and drive early iterations of crisis action planning. Today, the teams and their leaders do those things routinely, all while achieving so much more. Whether gathering intelligence, producing reports, driving targeting, or getting to the places we need to go, the members of our teams are second to none. It is impressive to watch different teams roll through our Joint Mission Operations Centers (JMOC) and accomplish the tasks at hand.

Speaking of JMOCs, what was once a single-room operations floor in building 310R ('leaky trailers'), is now a franchise of JMOCs across two sites in Maryland, two sites in Georgia, and a location in Hawaii. We work seamlessly with the JMOC in Texas and USCYBERCOM's JMOC-Enterprise. The success in our JMOCs is a function of the hard work of a couple of people early on and continuous rotations of TFE. TFE's efforts to defend and reinforce the infrastructure have truly enabled the brigade, U.S. Army Cyber Command, and USCYBERCOM. Many thanks to the men and women of the early iterations of TFE. This month we say farewell to TFE V; they have done a phenomenal job maintaining and improving operational infrastructure while constrained by COVID protocols. The next twelve months will be pivotal in the JMOC as the new TFE VI arrives and supports the transition of JMOC-Maryland to our Service partners.

Like the JMOC, the Cyber Solutions Detachment (CSD) has grown from a handful of developers into a well-coordinated group of talented people working in Maryland, Georgia, and Texas. The detachment produces for nearly anyone that has an Offensive Cyberspace Operations requirement. The CSD has developed for the Cyber National Mission Force, teams in the special operations community, the Army's Joint Force Headquarters – Cyber (JFHQ-C), and other services' JFHQ-Cs. The team developed certification exams for the different levels of proficiency. As a result, a work role that was shorthanded two years ago has thrived with the brigade's most sophisticated work-role management system. Many thanks to the incredible group of men and women who add exquisite capabilities to our team.

As it always has, the brigade will continue to evolve to meet the needs of ARCYBER and USCYBERCOM. Enabled by U.S. Army Intelligence and Security Command, we will continue to provide infrastructure and capability development well into the future. As always, change will happen. The 782d will add additional Teams. The 915th will grow to twelve Expeditionary Cyber Electromagnetic Activity (CEMA) Teams (ECTs) and continue to evolve how those ECTs support Army efforts in Multi-Domain Operations. In time, A Company, 60th Offensive Cyberspace Operations Signal Battalion, working in direct support of the brigade, will manage the operational infrastructures for the JMOC in Georgia. At the same time, TFE Soldiers will pivot to support emergent defensive operations. Finally, the faces around our organization will change. These endeavors will make the brigade stronger and more relevant in the future. The future will be exciting.

Many thanks to the Praetorian Soldiers, Civilians, and Families for the 'stuff and things' we have accomplished over the last ten years! Without your efforts, we could not have accomplished the incredible. You have contributed to our nation's ability to achieve 'silent victories.'

"Everywhere and Always…In the Fight!"

Respectfully,
Matthew Lennox
COL, CY
Commander, 780th MI BDE (Cyber)

780TH MILITARY INTELLIGENCE BRIGADE (CYBER)

HHC, 780TH MI BDE
HASTATI

781ST MI BN
VANGUARD

780th MI BDE
"STRENGTH AND HONOR"

915TH CWB
LEVIATHANS

782ND MI BN
CYBER LEGION

"EVERYWHERE AND ALWAYS... IN THE FIGHT"

Cyber Support Detachment to Cyber Solutions Development

By Capt. Evan Ames, D Company, 781st Military Intelligence Battalion (Cyber)

"We are defined not by the technologies we create but the process in which we create them." - Clarence "Kelly" Johnson, creator of Lockheed Martin's Skunk Works

WHEN I FIRST ARRIVED AT THE CYBER SUPPORT Detachment in August of 2017, the unit consisted of eight people working out of a portion of an old barracks building on the west side of Fort Meade, Md. That building, known as Hammerhead, housed all CSD: me, my 2nd Lieutenant BOLC (Basic Officer Leader Course) classmates, four First Lieutenants, three Captains, and a Major. The incumbent team had just completed a high-profile project that captured the attention of the Army Cyber community and was eager to exploit their success to grow their organization and take on bigger missions. The atmosphere was one of frenetic optimism. We knew that CSD was special, and our goal was to become the face of elite software and hardware development within the Army.

CSD's leader, then-Major (MAJ) Todd Arnold, had infiltrated the TRADOC-run Basic Officer Leader Course, under the guise of teaching a programming course. There, while he gave me and my classmates pointers on how best to use C, MAJ Arnold quietly marked down the lieutenants he thought could best contribute to CSD. A few months later, several lucky students found themselves holding PCS orders to the 781st Military Intelligence (MI) Battalion at Fort Meade. This means of operation was very much MAJ Arnold's style: when the bureaucracy won't work fast enough, shrewdly find a way around. Back then, CSD stood for Cyber Support Detachment, since CSD was a detachment under a company of the 781st MI Battalion (BN). MAJ Arnold initially tried to attach CSD directly under 780th MI Brigade (BDE), but administrative issues prevented that. Instead, CSD moved to instead exist within the Headquarters and Headquarters Company, 781st MI BN, and there it remained for the next few years.

CSD's mission profile in those days was diverse despite our small personnel roster. We worked on everything from radio hardware projects for boutique customers to the Army Platform Mission Assurance, a program through which the Army would ensure the cyber security of its major mission platforms. Temporary Duty Orders (TDYs) were a regular part of the mission, whether it was flying to Fort Hood, Texas to conduct a Cyber range, or to Redstone Arsenal, Alabama for a planning exercise. We worked in small teams and did not hesitate to multitask to train teammates on new techniques or avoid waiting on a slower project.

Despite what I was told to expect by TRADOC (U.S. Army Training and Doctrine Command), I rarely observed a formal Cyber requirement process in those days. Our projects were largely based upon personal requests and favors exchanged among Army Cyber leadership, and we often formalized requirements long after we had begun working on deliverables. We were quick and motivated, but we had not yet grown the critical organizational structures and procedures necessary to make our performance scalable and repeatable. There was nothing wrong with this at the time, since the organization was so small as to not benefit from such factors, but we would need to change in order to scale the organization and take on more and larger projects.

Our development environment and computer network likewise reflected our priorities and attitudes. In the Hammerhead days, we maintained an ad-hoc network of scavenged hardware upon which to conduct our development activities. Individuals set up and hosted internal services like a Gitlab server and Linux repository mirrors from their development machines. If the internal Pip mirror went down, we could put in a ticket to solve the problem by shouting down the hallway "Hey Dave, what did you do? The Python repo mirror is down again!" When we wanted to get some software from the outside internet, we (gasp!) used removable media. In those days, our work was limited to Unclassified work only, of course. This, too, would change as the organization grew and our scope of work widened.

Cyber Solutions Development (CSD) took its first major steps away from ad-hoc cowboy-style development with the arrival of the second lead developer, Lt. Col. (LTC) William Michael Petullo. CSD was still a detachment under HHC 781st and had since added a graduating class of TDQC (Tool Developer Qualification Course) and about a dozen other Soldiers to its ranks. With about 30 people on the books, CSD-M's (Maryland) quick and informal management style struggled to keep up. I write "CSD-M" because by this point, CSD-G (Georgia) had also been created under the 782nd MI BN at Fort Gordon, Georgia.

I distinctly remember LTC Petullo's vision speech, in which he compared the amorphous structure of early CSD to a jellyfish and the purpose-driven, efficient

future of CSD to a shark. To complete this metamorphosis, CSD would need to develop the distinct tissues and structures necessary to give it strength and speed at the cost of flexibility. We would organize into teams specialized for particular mission sets. We would develop an advanced digestive system, formalizing our requirements acceptance and product delivery processes. Most importantly, we would devise a lifecycle of cellular development, by which more senior developers would mentor and nurture junior ones. This speech betrayed the incredible level of planning that LTC Petullo had put into moving CSD forward under his watch.

In the next few years, the situation played out almost exactly as LTC Petullo initially described. CSD continued to grow its CSD-G detachment and added CSD-TX (Texas) and CSD-T (Tactical), and CSD-H (Hawaii). Promising enlisted Soldiers continued to work through TDQC, and some Soldiers, like me, went through other training pipelines. Under U.S. Army Cyber Command (ARCYBER), CSD worked to create a generalized basic developer exam along with senior developer exams specific to different skill areas. These exams were published in tandem with JQRs, or Job Qualification Requirements, which would guide prospective developers when studying to certify in their area of excellence.

Just as the developer certification process gained scope and structure, so did our developer network and working environment. About a year after LTC Petullo took command of CSD, the entire organization picked up everything and moved to an office building outside of Fort Meade. 780th MI BDE and 781st MI BN initially planned to only move CSD, but later decided that the entire 781st MI BN headquarters (HQs) would also relocate. The CSD-M Developers, now numbering several dozen, occupied cubicle farms in two separate rooms of the building and would exist within personnel billets for D Company of the 781st. At the same time as the move, CSD transitioned to a more centrally administrated developer network, RCDN. CSD could now spend most of its time focused on development, rather than maintaining its own network and infrastructure.

Following and building upon the legacy of LTC Petullo, MAJ Micah Bushouse took command of CSD in early 2020. Where other lead developers had focused on building and spreading the structures and processes of CSD, MAJ Bushouse's tenure worked to consolidate disparate processes and organizations to centralize the organization. MAJ Bushouse pioneered the Multi-Functional Crew DevOps concept, through which a developer crew worked at 780th MI BDE HQ to directly support customer operators. MAJ Bushouse's tenure also saw the creation of the 17D MOS for Cyber Officers, providing a unified MOS to distinguish Cyber Developer Officers in the Army's eyes. He also oversaw the creation of the CSD directorate, consolidating the leadership of each CSD site under 780th MI BDE.

The most recent Lead Developer, MAJ Charles Suslowicz, took command of CSD only a few months ago. Like each of the prior Lead Developers, he formerly served as an instructor and researcher at the United States Military Academy and holds an advanced degree in a Computer Science-related topic. Under his leadership, D Company, 781st renamed itself the Daemons, reflecting the long-term home of CSD-M within the unit. I look forward to the other changes and improvements MAJ Suslowicz will make to CSD over the next few years.

The character and tone of CSD have changed dramatically since I first arrived. CSD evolved from a team focused on relatively high-risk, high-reward operations to a more mature, process-driven unit. CSD's leaders established pipelines to create and grow qualified personnel, generate mission requirements, and deliver products to customers across the Department of Defense. They successfully scaled the organization from an ad-hoc detachment of motivated hackers into a directorate of development professionals prepared to support the needs of the Army. I do not know for certain what the future holds for CSD, but I have confidence that its skilled and motivated leadership will continue to develop it for the better. ■

FORT GEORGE G. MEADE, Maryland - A new chapter was started for the Army presence in cyberspace when the 780th Military Intelligence (MI) Brigade officially organized a provisional Cyber Solutions Development (CSD) detachment under the 781st MI Battalion at Club Meade on July 25, 2017. In a ceremony steeped in military tradition, the detachment's guidon was uncased for the first time and then-Maj. (MAJ) Todd Arnold, the Army officer who led the effort to make this vision a reality, passed the guidon to the incoming officer in charge, then-MAJ W. Michael Petullo.

What's in a motto?

By Chief Warrant Officer 3 Justin Helphenstine, D Company, 781st Military Intelligence Battalion (Cyber)

Thoughts on the nature of the Brigade, and what the next ten years could hold

THE 780TH MILITARY INTELLIGENCE BRIGADE (CYBER) is unique among Army formations. Its designation as a Military Intelligence Brigade evokes the joke about the Holy Roman Empire – neither Holy, nor Roman, nor an Empire. The bulk of our assigned personnel do not present the Service or the Combatant Commands with a Military Intelligence capability. We do not fight as a Brigade, have no wartime mission for Decisive Action in support of Unified Land Operations, and answer to both the Army Service Component Command for United States Cyber Command (USCYBERCOM) as well as U.S. Army Intelligence & Security Command (INSCOM).

I joined this formation in 2009, and over the years have participated in enough bull sessions to hear the same refrains sung anew as each wave of incoming personnel asks questions about the seeming oddities of the 780th. I would like to take this opportunity to share what I have learned about "why things are as they are." Following this, I will lay out three things I believe the Brigade can do to play to its strengths and generate the elite force we need for the next ten years.

Let's start at the very beginning, it's a very good place to start. Department of Defense Directive 5100.01 defines the functions of the Department of the Army. "The Army shall contribute forces through a rotational, cyclical readiness model that provides a predictable and sustainable supply of modular forces to the Combatant Commands, and a surge capacity for unexpected contingencies."[1] Contributing forces first requires generating forces. Force Generation is the Army's core function.[2]

To accomplish this, most of the Army is assigned to "MTOE units" – "Modification of Tables of Organization and Equipment", though I think of them as "Maneuver" or "FORSCOM" units. These are the main focus of the Army's Sustainable Readiness Model – the provisioning of forces for decisive action in support of unified land operations.[3] The alternative to MTOE is a TDA, or "Table of Distribution and Allowances"; the 780th is a TDA unit. You can browse these tables via the FMS Web portal[4]; this portal is provided by HQDA G-3/5/7, also the proponent for AR 525-29. It's a terrific career planning resource, allowing you to see the distribution of your MOS and grade across the Army (and Joint) formations.

MTOE units operate on Unit Deployment Cycles, transitioning through states of preparation and readiness for deployment. Units not participating in SECDEF-designated deployments instead use the Unit Readiness Cycle. Both type of Cycles are exactly that – cycles – implying a transition between preparation and readiness. Through these cycles, the Army executes its core function of Force Generation. Readiness allows a unit to be marked "available" for operational employment by a Combatant Command (CCMD), such as USCYBERCOM, or US Central Command.

Soldiers assigned to the 780th are typically rostered onto Cyber Mission Force teams. These teams are assigned to USCYBERCOM, which includes all active and reserve cyber operations forces in the armed forces stationed in the United States, unless otherwise assigned.[5] Teams are assigned in perpetuity, leading to the dual identity of every Soldier (and 780th Civilian) assigned to a team, as both operationally subordinate to the Commander, USCYBERCOM while administratively subordinate to the Commanding General, INSCOM. This dual identity represents the most significant property of the 780th for anyone seeking to understand "why things are as they are."

Recall that the Army is built to execute Force Generation – one of the three core military tasks (the others being Force Projection and Force Employment), and alone bears the burden for generating Army capabilities.[6] The Army has developed a rich set of frameworks, models, and business processes to accomplish this task. Many of those processes, operating on a years-long timeline, worked to bring you here. As noted earlier, the Army is tasked with providing forces through a rotational, cyclical readiness model. We don't do that in the 780th, though, owing to teams' continuous assignment to USCYBERCOM.

Mission teams do not participate in SECDEF-recognized deployments. Nevertheless, they are deployed de facto, through assignment to a CCMD, in perpetuity. No mission team has been reassigned to the Service from USCYBERCOM. Every one of our mission teams is in the fight, night in, night out. This is grounded in DOD Directive and reflected in our heraldry, "Everywhere and Always…In the Fight".

Soldiers assigned to a team can spend a three-to-five-year tour under Operational Control (OPCON) in the CMF. OPCON commanders execute another one of three military force operations – Force Employment. This explains why you should never expect the CNMF Commander to cycle out a National Mission Team for a quarter to train for the future fight: it's their job to employ

forces to meet objectives identified in the Guidance for Employment of the Force.[7] They are the consumer in a producer-consumer model first established in the Department of Defense Reorganization (Goldwater-Nichols) Act of 1986, which astute readers may recognize as preceding the establishment of USCYBERCOM.

Let us pause and take stock of what we have covered. First, the Army is charged with Force Generation, and has robust business processes to do that. These processes execute on forces before and after they are presented to a CCMD. Secondly, our forces are continuously presented to a CCMD, and are not projected to exit the "Mission" phase to return to Preparation or Readiness, as laid out in AR 525-29.

Conclusion: The Army has business processes to generate forces and achieve Sustainable Readiness, but our unit is not structured to execute them.

There is no "770th MI BDE" waiting to relieve us, nor is one projected. Our mission teams are, for the foreseeable future, the totality of the Army's (conventional) Offensive Cyber Operations elements. I don't believe that's the end of the story, though; I think there are ways, grounded in doctrine, for the 780th to evolve into the sine qua non of an elite offensive cyber force. Like all good briefers, I have brought three ideas with me to carry us from where we are to where we want to be.

First, I encourage the 780th to change how we tell our readiness story. We presently use C-level ratings, "which are an overall measure of a unit's training, personnel, and equipment assessments, reflect(ing) a unit's ability based on organizational design to provide core functional capabilities".[8] Units in "receipt of an assigned mission" use A-level ratings to assess Assigned Mission Manning, Equipment, and Training. "For A-level, commanders evaluate training, personnel, and equipment availability carefully tailored to reflect the unique requirements of the mission".[9] Telling the story of readiness tailored to the teams' unique missions can send the demand signal for specialty training or manning. As an example, consider a fictional mission team whose aligned targets are better approached through a focus on the persona layer vs the logical layer. CMF 17 does not specialize here, but CMF 37 may be of significant value.

Speaking to Assigned Mission Manning could tell this story better, in contrast to the C-ratings for a stock company in an MI Brigade.

The second focus for the future should be on securing the ability to execute Force Generation. While our forces are assigned (through teams) to USCYBERCOM, the Commander, USCYBERCOM's duties include the responsibility to organize, train, and equip cyber operations forces in coordination with the Military Service Chiefs.[10] These duties imply a Force Generation, as well as Force Employment, responsibility, and the Brigade should be the preferred partner for commander USCYBERCOM in generating Army cyber forces.

Enabling Force Generation requires shifting from a singular focus on Force Employment. The need to better balance Generation with Employment is not new to the Department of Defense. Writing in

early April, members of the House Armed Services Committee addressed Secretary of Defense Lloyd Austin and Deputy Secretary Kathleen Hicks: "The 'tyranny of the now' is wearing out man and machine at too high a rate to ensure success both now and later. Future readiness can no longer be sacrificed at the altar of lower priority requirements."[11]

Quartering in the quotidian yields quotidian quality. The all-consuming commitment to the current moment deprives us of the chance to match, let alone best, our adversaries. Accordingly, our EAs (exploitation analysts) and Operators should rotate out from their Mission Teams for one year out of every three. This will provide the Brigade with meaningful time to grow this force. I see a plethora of possibilities to accomplish this, from individual training to internships, from integrating with the NSA's workforce to touring through the JMOC (Joint Mission Operations Center). Two realities underscore the need for the 780th to have more opportunity for Force Generation: we have not mastered offensive cyber, and the mission teams are not chartered to do so. Rotational assignments would signal recognition by the Army and Joint community that persistent engagement is more than "fight tonight, every night."

Lastly, and most crucial to our evolution, the 780th should lead the charge in rendering today's 10-level tasks into tomorrow's automated workflows. Between our engineers at the JMOC and our capability developers in CSD, the brigade has the manning to aggressively automate many operator and analyst tasks. This automation elevates our constraint, freeing up operators and analysts to focus on their mission. For operators, it means abstracting blue and gray space, as well as abstracting 'mounting weapons on the wings'; when an operator recognizes a need for a capability, it should be seamlessly available, provisioned on-demand. For analysts, it means workflows and tooling which enable comprehending the totality of target entity. Crucially, this supports achieving shared awareness across the mission team. Commanders, planners, and analysts should be able to discuss targets as easily as maneuver commanders, FIRES planners, and all-source analysts do in the terrestrial domain; analysis and visualization tools are vital to enabling this. These goals may sound lofty, but they address problem sets at the fore of the domain. Aggressively developing these solutions brings us online with industry and adversaries and offers the Brigade greater operational purpose.

The 780th has structural tensions arising from its identity as a Service-retained element administering forces permanently assigned to a CCMD. Our Soldiers and Civilians in the CMF are deprived of time in the "generating force" and the chance to benefit from the Army's robust business processes for Force Generation.

The Brigade has a duty to signal this abnormality to the Army and Joint community. This begins with using appropriate readiness measurements to speak about manning, equipment, and training gaps for teams' assigned missions. The Brigade is also charged with growing its Soldiers and Civilians, and this requires periodically cycling them out of current operations. The lived history of the 780th shows us the costs to modernization efforts incurred by a relentless focus on reacting to the adversary's last move.

Finally, the 780th has the means to aggressively automate workflows for both operators and analysts, elevating our constraints and ensuring their mental energy remains focused on those challenges only they can tackle. These three initiatives represent further evolution for the Brigade and should come to define what it means to be "Everywhere and Always…In the Fight."

References:

1 DODD 5100.01, "Functions of the Department of Defense and Its Major Components", p. 34

2 AR 525-29, "Force Generation - Sustainable Readiness", 1 October 2019, p. 3

3 AR 525-29, p. 25

4 See https://fmsweb.fms.army.mil

5 DODD 5100.01, p. 28

6 AR 525-29, p. 2

7 AR 525-29, p. 36

8 AR 525-29, p. 24

9 Ibid

10 DODD 5100.01, p. 29

11 Letter from members of the House Armed Services Committee to Secretary of Defense Austin and Deputy Secretary of Defense Hicks, 5 April 2021, retrieved from US Naval Institute: https://news.usni.org/2021/04/05/house-lawmakers-want-pentagon-to-rethink-global-force-deployments


780TH MI BDE (CYBER)
781ST MI BN
PRAETORIANS
GUARDIANS
HHC 781ST
STANDING READY!
ETERNALS
ALPHA COMPANY
AVENGERS
UBI CETERI NON POSSUNT
DELTA DAEMONS
BRAVO IMMORTALS
NUNQUAM FEROCIAM
Conquerors
VANGUARD
"WHEN OTHERS CANNOT"

Advanced Individual and Collective Training: Foundations for Maintaining a Competitive Advantage in Cyberspace

By Christopher J. Rudy, A Company, 782nd Military Intelligence Battalion (Cyber)

OVER THE PAST TEN YEARS, the 780th Military Intelligence Brigade (Cyber) has been focused on manning, training, and equipping Army cyber mission teams in support of U.S. Cyber Command (USCYBERCOM) and U.S. Army Cyber Command (ARCYBER) mission requirements. Early on, the focus was on standing up mission teams, training Soldiers and Civilians in their cyber work roles, and enabling the teams to achieve initial operating capacity (IOC). IOC required mission teams to be filled to specific levels with a defined number of personnel trained and certified in their work roles. Training largely focused on ushering personnel through partner agency-provided pipeline training. Mission teams also embedded their personnel with our partner agency to learn tradecraft and gain valuable experience.

As teams achieved IOC, the focus shifted towards enabling mission teams to reach full operating capacity (FOC). FOC required teams filled to increased levels with increased on hand personnel trained and certified. FOC also came with a requirement of successfully completing a certification event. To meet this requirement, the Brigade developed the first collective training exercise, which effectively incorporated all sub-elements and work roles on a mission team. This collective training exercise served as a key certification event for all Army Combat Mission Teams (CMT) and Combat Support Teams (CST) moving forward. Lessons learned from the FOC event created the Operational Readiness Assessment (ORA), which continues to reassess the readiness of all Army CMTs and CSTs. The Brigade also invested heavily in building a virtual training environment to facilitate a more realistic training experience. Lessons learned from using this virtual training environment shaped the development of the Persistent Cyber Training Environment currently used by the joint force for cyberspace collective training.

The Brigade began to increase emphasis on getting beyond pipeline training, upskilling, and exceeding USCYBERCOM certification requirements. The Brigade initiated a Technical Health Working Group (THWG) to bring experts from each work role together to provide updates and recommendations for improving training for each work to the Brigade Commander. The THWG morphed into the Work Role Working Group (WRWG) and was adopted by ARCYBER. The ARCYBER WRWG drafted new Army Joint Qualification Requirements (JQR) for each work role, updating the JQRs to provide cyber focus and depth required to distinguish basic, senior, and master proficiency levels. ARCYBER presented the JQRs to USCYBERCOM J7 for incorporation into the joint standard. Additionally, the Brigade increasingly augmented pipeline training with vendor-provided industry training.

As the Brigade operationalized with the standing up of the Joint Mission Operation Center and Capabilities Support Detachment (CSD), training requirements evolved to address new mission requirements. Not only was the Brigade responsible for ushering mission team personnel through pipeline training and JQRs, it was now responsible for training and certifying personnel on service-specific tools and capabilities. The Brigade led the development of the Tool Development Qualification Course for training new Army capability developers to support the growth of the CSD. Furthermore, the Brigade provided instructors and course writers to the Army Cyber Center of Excellence to assist with developing and training the new Basic Operator Course, which was vital for growing the cyber operator pool required to support the increasing mission requirements levied on the cyber mission force.

As we shift focus from the Global War on Terror to Great Power Competition, the need for individual and collective training will continue to increase. Our adversaries are growing more capable, and their tactics are always evolving. Continued commitment to providing advanced individual training to tenured personnel is just as important as providing pipeline training to new personnel. There is increasing emphasis on elevating more personnel to senior and master proficiency levels to maintain competitive advantage. The services are becoming more responsible for training its personnel internally and the Brigade must grow more adjunct faculty instructors to meet pipeline-training requirements. Warrant Officers, Non-Commissioned Officers, and Civilians must also take on a larger role with training our force. Furthermore, we must make increased use of Sergeants Time Training, on-the-job training, and mentorship programs to train new personnel and ensure new tactics, techniques, and procedures shared throughout the community.

Collective training continues to be critical for maintaining our competitive advantage. In addition to assessing readiness, it serves to reinforce individual training and standard operating procedures. Collective training events provide mission teams the opportunity to execute a cyber-mission from receipt of mission to executing effects while in a time constrained crisis action environment.

What takes one to two weeks to accomplish during a collective event, may span six months to two years while conducting real world mission. If conducted early in their tenure, collective training sets new team leads up for a successful tour by providing team leads an understanding of the full capability of their team. It also serves to re-energize teams who could otherwise become stagnant working the same mission year after year. With that said, our scenarios have been in use for over five years and are due for a refresh. We also need to grow the assessor pool as many of our long-time assessors have transitioned to new formations or careers.

When it comes to cyber operations, people are our most important resource. Continuing to invest time and resources to ensure our people are the most trained and ready force in the world will ensure the United States maintains a competitive advantage in cyberspace. To that end, the 780th MI BDE is always looking for volunteers to help develop new training scenarios, serve as assessors for Battalion and Brigade training events, serve as JQR trainers and evaluators, and become adjunct faculty instructors for critical work role training. It takes motivated personnel with recent experience on mission teams to make training and scenarios more realistic and worthwhile. While there is a cost to you and your team with regards to time away from mission, it is well worth the cost. Your efforts greatly improve the cyber mission force and you and your team benefit from lessons learned by assessing and training other people and teams.

FORT GEORGE G. MEADE, Md. -- Gen. Charles Q. Brown, Jr., Chief of Staff of the Air Force, speaks with Cyber National Mission Force members about full-spectrum cyber operations during his visit to U.S. Cyber Command, at Fort George G. Meade, Md., May 10, 2021. The visit provided the opportunity to engage with cyber experts about their unique missions, designed to create competitive advantages in cyberspace. (Photos by Josef E. Cole III)

Company Grade Officers Filling Technical Roles

By Capt. Andrew W. Moss, Detachment-Texas, 782nd Military Intelligence Battalion (Cyber)

"NEEDS OF THE ARMY." It is a saying we all know and have quite often heard throughout our careers. A specific need of the Army is a requirement to fill technical roles. The Army is in desperate need of any rank, enlisted or officer to take on the challenge of becoming certified in a technical role. Army Cyber is seeking all MOSs to apply, does not matter if you are enlisted, an officer, or civilian. The Army will consider anyone that qualifies. But, why should Officers be technical, aren't they supposed to be leaders? What makes up a leader and can a leader be technical? There are a few paths an officer can take to gain leadership experience.

The Army in late 2017 started the "Army Cyber Direct Commissioning Program", in order to recruit "civilians with specific high-demand technical skills to join the Army as commissioned officers." The Army is already identifying the need for technically skilled individuals to populate the ranks of officers. This is a fantastic opportunity for individuals to join the Army with professional civilian experience. The question is how to use these individuals correctly. Do you keep them in managerial roles, or use them in technical roles? The Army already identified a need for highly technical officers to join their ranks, but how do we utilize them correctly?

Army Cyber as a branch needs to stop looking at traditional leadership roles as how many people we rate, but by the impact that specific role serves. There are many reasons an officer could fill as the Director or Deputy Director of Cyber Tactical Operations Center (CTOC), Weapons and Tactics Director, or Weapons and Tactics Lead for a "Key Developmental" (KD) role. Both positions fill a leadership role of mentoring others, managing operations, and assuming risk. General Colin Powell once stated, "Leadership is solving problems. The day soldiers stop bringing you their problems is the day you have stopped leading them." Not a day goes by that a Soldier doesn't come talk to me about a certain problem set and requires guidance or help. This is a prime example of the conundrum we face in Cyber, or should I say the Paradox of Army Cyber (PAC).

The PAC is a self-created problem the Army faces in today's ranks. The Army develops junior officers to be leaders, managers, and eventually assume command at the same time the Army is creating officers to be technical experts. They both fall in the same MOS as 17As but are both expected to compete on the same level. One solution for this issue is to create two separate MOSs for officers. One to follow the traditional Army leadership career path, and the other to experience the technical expert career path. This could help alleviate the problems they will face (managerial leaders in a technical field) in the future while developing what it means to be a leader of technical experts by separating the MOS (Cyber Management and Cyber Operations).

They would both have their own professional military education courses (PME) for their respective ranks. This would allow an individual to focus on Management or Operations to identify different progression tracks and allow them to be trained separately and specifically to their career goals. This would allow the Army to create different training companies for each different MOS to have their own requirements to be filled. Mentors integrated within these companies to help guide future junior officers transition into their work roles.

Identifying and acquiring technical officers from the beginning of basic officer leadership course (BOLC) and transitioning them to a training company relevant to a technical role could be the first step. Once at the training company they go on to the extensive training pipeline that follows, having mentors that are integrated within the company can provide guidance and help transition them for their first duty station. After successful completion of their training, they convert into the new MOS for being a technical expert. This MOS would allow them to obtain the required KD to be competitive for promotion. When they go to Captains Career Course, they could have the option of converting back to a 17A and continue the rest of their career with the normal traditional officer route or have another chance when they go to ILE as a Major. Same as in reverse; allow a Captain to qualify for the technical MOS and go to the training company to go through the pipeline. We should give options to our soldiers, allow them for future success in a dynamic career field of Cyber.

References:

[1]*ARCYBER HQ Website." ARMY CYBER FACT SHEET: Army Cyber Direct Commissioning Program" (Feb 2018). Available at https://www.arcyber.army.mil/Info/Fact-Sheets/Fact-Sheet-View-Page/Article/1440683/army-cyber-fact-sheet-army-cyber-direct-commissioning-program/*

[2]*GEN Colin Powell and Joseph E. Persico. My American Journey. New York: Random House, 1995. Print*


780TH MI BDE (CYBER)
782ND MI BN
PRAETORIANS
HHC
782nd MI BN
SUPPORT THE FIGHT!
DETACHMENT TEXAS
CYBER RANGERS
CYBER LEGION
SILENS VICTORIA
CYBER ARCHERS
KOHANAS
birds of prey
oculus aquilae
C CO
CENTURIONS
LEAD THE CHARGE
DRACONES
BURN IT DOWN
Cyber Legion
"Silent Victory"

The 915th Cyber Warfare Battalion: Evolving to Fight Multi-Domain Operations

By Capt. Gabriel Akonom, Headquarters and Headquarters Company, 915th Cyber Warfare Battalion

THE 915TH CYBER WARFARE BATTALION (CWB) is the first and only battalion of its kind in the United States Army.

The unique capabilities of the 915th CWB distinguish it from other cyber units. A force designed to be expeditionary, the 915th CWB can deliver a range of non-lethal, non-kinetic effects from offensive cyberspace operations and electronic warfare (EW) capabilities. The ability to get close to targets, which would be inaccessible remotely, makes the 915th CWB essential in performing many unique roles. These roles include developing ways to infiltrate enemy anti-access and area denial (A2AD) networks and extending enterprise and national capabilities at the tactical level. At the cutting edge of information advantage operations, the 915th CWB readily provides non-lethal, non-kinetic effects to designated Army Service Component Commands (ASCCs) and their designated subordinate elements to achieve decision dominance.

Command Sgt. Maj (CSM) Marlene Harshman, former member of the Cyber Support to Corps and Below (CSCB) pilot program and current 915th CWB senior enlisted leader, witnessed the full evolution of the battalion.

"We train hard, educate the force, and build relationships for future operations and opportunities," said CSM Harshman. "Our Soldiers are fully trained cyber and electronic warfare experts and professionals, standing by and ready to support."

The 915th CWB was not always the CWB we know today. Since its inception, the expeditionary cyber electromagnetic activities (CEMA) force had several growth periods. Each phase was accompanied by a unique purpose, mission, and operational focus. The concepts of expeditionary cyberspace operations have evolved, and the force has been steadily growing their capabilities and notoriety, reinforced by many successful, and in some cases, first-ever training events.

The Cyber Support to Corps and Below (CSCB) Pilot Program

The CSCB pilot program began in 2014 as an effort by General Odierno, the 38th Army Chief of Staff, to integrate cyberspace operations into the maneuver battleground at the tactical level. In 2014, it was unknown how useful cyberspace operations would be to brigade combat teams (BCTs). Furthermore, no precedent existed to understand what combination of personnel and equipment this type of unit would need. Lastly, the Army did not know how the force would need to adapt to fighting in a digital domain. The intent of the CSCB mission was to provide an answer to these questions. The early CSCB was comprised of Soldiers and Civilians from 780th Military Intelligence Brigade (MI BDE). The CSCB began their support to the Combat Training Centers in the first ever Joint Readiness Training Center (JRTC) 15-07 rotation followed by the National Training Center (NTC) 16-08 rotation. These rotations began expeditionary cyberspace operations.

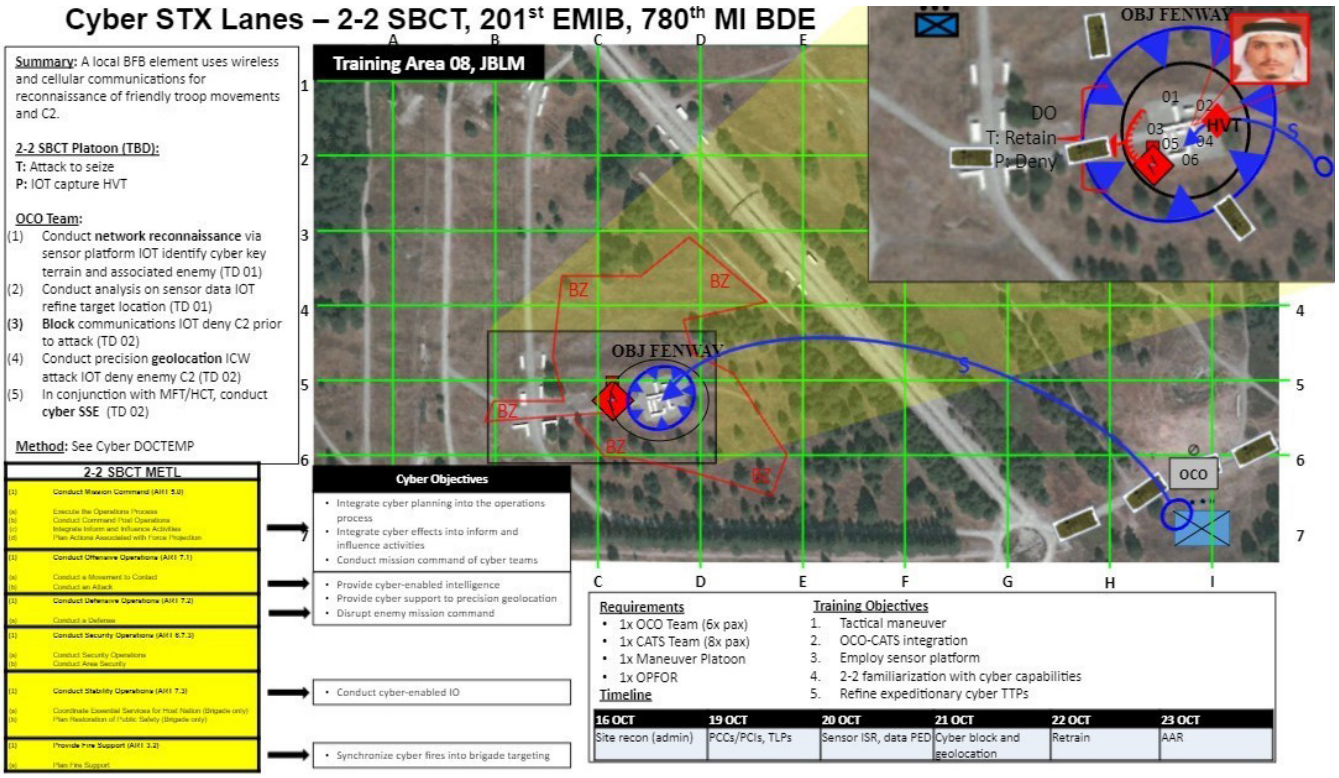
From left to right: Chief Warrant Officer 3 (CW3) Nevery Berry, Sgt. (SGT) Osvaldo "Alan" Solis, Staff Sgt. Nicholas Davis, and Sgt. 1st Class (SFC) Christian Bratcher during JRTC 15-07. Courtesy of CW3(Ret.) Nevery Berry. Ranks reflected at the time of event and picture.

From right to left: Capt. Sally White, SFC Brian Fife, SFC Matt Varney, SFC Marlene Harshman, SGT Niterson Laplante, Specialist James Campbell during NTC 16-08. Courtesy of Maj. Sally White. Ranks reflected at the time of event and picture.

In the early years of the CSCB, the training effort was split between integrating into BCT planning cycles, teaching BCT staffs how to effectively integrate cyberspace operations into their own planning, modifying CTC programs to reflect accurate cyber situations, and developing from expeditionary cyberspace capabilities.

"The lack of resources for capability development was a particularly acute problem," said Maj. (MAJ) Sally White, the commander and team lead of the NTC 16-08 rotation. "For the two CTC rotations I was involved with — JRTC 15-07 and NTC 16-08 — we had to rely on a combination of antiquated Army capabilities and open-source devices that some of our lieutenants had thrown together [during] their off time."

At that time, there were no Mission Essential Tasks (METs) for the CSCB to train from, no Gunnery Tables, and no doctrine to reference. The CSCB pilot program focused on creating the framework for future units by integrating early in the planning process of supported units, collecting lessons learned, developing growth requirements to increase capability, and worked closely with TRADOC's Doctrine, Organization, Training, Materiel, Leadership and Education, Personnel, Facilities and Policy (DOTMLPF-P) team. The early CSCB successes affirmed the Army's decision to create a dedicated Expeditionary Cyber unit. The training events conducted by CSCB include several Brigade FTXs, situational training exercises, home station training (HST) events, warfighter exercises, JRTC rotations, Joint Multinational Readiness Center rotations, and NTC rotations.



CONOP (Concept of Operations) from HST with 2/2 Stryker BCT while preparing for NTC 16-08. Courtesy of CSM Marlene Harshman.

The Expeditionary Cyber Support Detachment (ECSD), 782D MI Battalion

In response to HQDA EXORD 153-17, the 782D MI Battalion (BN) established the ECSD to continue the CSCB pilot initiative. The ECSD mission was to execute offensive cyber operations (OCO) in support of what was renamed to CEMA Support to Corps and Below (CSCB) with the task to defeat the enemy, enable force protection, provide indications and warnings, and create rapid collection of information at the tactical level. A staggering number of eleven division and brigade evaluation exercises occurred during ECSD's tenure, each event building on the lessons from the previous iterations. At this point in the CSCB pilot program, the ECSD joined forces with ARCYBER elements, 780th MI BDE experts, 1st IO (Information Operations) Command, and the Cyber Protection Brigade to provide a full spectrum of capabilities. The ECSD effectively continued the CSCB efforts to craft a strong framework for the future of expeditionary cyber operations.

"780th's collection and refinement of the ECSD's after-action review comments drove decision-making at ARCYBER, who synthesized the data into a recommendation for the organization and composition of a Battalion-sized element focused on mission tailored CEMA support to Army Service Component Commands and Theater Army, eventually manifesting in the 915th Cyber Warfare Battalion," said Capt. (CPT) Adam Schinder, a former ECSD Team Lead.

ECSD Soldiers during Lightning Forge 18-01. Courtesy of CPT Adam Schinder.

Training in the ECSD had the benefit of some prior experience achieved during the early years of the CSCB. Additionally, ECSD had the continued support of 780th MI BDE experts and their shared tactics, techniques, and procedures. The training effort was more focused and intentional, while continuing to use the DOTMLPF-P assessments to formalize feedback. Understanding the need to fully integrate into maneuver units, the detachment place significant emphasis on physical fitness and tactical training. Additionally, the ECSD was equipped with an internal rapid development team that not only quickly developed hardware solutions to inherent problems while conducting expeditionary cyber operations, but also developed hardware and software training environments and adversary networks to accurately simulate real-world components. The development team enabled the creation of cyber training scenarios and extended the detachment's ability to integrate cyber capabilities into CTC rotations and division-level training events. Additionally, this training model was significantly more effective in allowing Combatant Commanders to see the tangible effects of the integrated CEMA capabilities. The battlefield effects were evident due to the extensive planning and staff integration the CSCB team provided. Building on the lessons from the CSCB pilot, the ECSD was fully equipped to provide expeditionary cyberspace infrastructure support crews to CTC Exercise Control, as well as expeditionary OCO plans crews and expeditionary OCO crews to the supported brigade. Integrating this cyber expertise into the planning cycle dramatically increased cyberspace success during these exercises, but also vastly illuminated the value of cyberspace operations to the tactical commanders. These functions were arguably more valuable to the future success and integration of follow-on units. ECSD supported a multitude of exercises, to include NTC 17-06 with 2/1 ABCT, NTC 17-07.5 with 1/4 SBCT, NTC 18-03 with 1/4 SBCT, NTC 18-08 with 3/1 ABCT, NTC Leader Training Program with 3/1 CAV, Cyber Blitz 2018, NTC 19-03 with 3/1 CAV, and a COMMEX at JMRC for Saber Junction 19 with 173rd IBCT.

The 915th CWB and the Expeditionary CEMA Team (ECT) Concept

Army Cyber established the 915th CWB based upon the feedback and results from the CSCB and ECSD lessons learned. The 915th CWB was designed to be the dedicated, service-retained, scalable expeditionary cyber force to meet the needs of fighting future conflicts. By fiscal year 2026, the 915th CWB will have 12 ECTs, each capable of providing OCO, EW, and information advantage functions and capabilities. Each ECT consists of two expeditionary firing crews, two remote firing crew, a plans section, an infrastructure support element, and have capability development support. The CWB mission is to conduct information advantage operations to designated Army Service Component Commands (ASCCs) and their designated subordinate elements. However, unlike its predecessors, the 915th CWB is neither an assessment venture nor training aid. The 915th CWB is the first dedicated battalion capable of providing integrated expeditionary cyber capabilities—culminating the years of hard work and development of the vision that began in 2014.

Originally, the 915th CWB began to build upon the experience of its predecessors and continued supporting CTCs rotations with an emphasis at the BCT level. However, as the scope of future conflict has become clearer and with the Army's renewed emphasis on Large Scale Combat Operations (LSCO), the 915th CWB's focus shifted. MAJ Richard Byrne, 915th CWB S3, helped established the first ECT.

"When we first stood up ECT-01, we were a team of less than 15 Soldiers. Our first task was to execute a CSCB rotation with the 173rd ABN (Airborne) BCT at Saber Junction 19, Hohenfels, Germany. The 1st ID was providing the higher headquarters element for the 173rd BCT during SJ19," said MAJ Byrne. "We initially struggled to synchronize the ECT's capabilities with the 173rd BCT and we quickly realized how important the Division echelon was for synchronizing enablers during a tactical maneuver. At the Division Level, the 1ID CEMA Cell was able to integrate our effects in a meaningful way. The Division AO was much larger at the Division level, and they were concerned with targets that had strategic impacts. It became clear that a Division was ideally the lowest echelon of unit we could practically integrate with. As we gained more experience supporting Divisions, Corps, and sometimes SOF [Special Operations Force] elements the concept of employment for ECTs matured."

While ECTs still support echelons of various size throughout the battlespace, experience demonstrated that the detailed planning and targeting started with larger staffs.

A key partner for the 915th CWB in future LSCO is the Multi-Domain Task Forces (MDTF). The Army created the MDTF to focus on the five objectives (compete, penetrate, disintegrate, exploit, re-compete) of Multi-Domain Operations (MDO) during LSCO. The 915th CWB has built relationships and partnerships to fill critical gaps in the capabilities supporting the MDTFs through planning, coordination, employment of EW capabilities, and integrating OCO into the MDTF's targeting cycle. These capabilities support both lethal and non-lethal fires allowing Expeditionary CEMA Teams (ECTs) to have a layered presence throughout each echelon of the battlefield as the MDTF competes and operates to project power through adversary A2AD (anti-access/area denial) networks.

Defender Pacific 2021 affirmed integration with the MDTF. Defender Pacific 21, executed by ECT-01 in Guam, was the first time the ECT deployed with the MDTF to synchronize and integrate CEMA capabilities into their planning processes. ECT-01 was able to support the MDTF with spectrum analysis and provide a more in-depth understanding of cyber capabilities that would support the development of future CONOPs in support of the MDTF and the ASCC.

"ECT-1 was our most significant external asset during DP'21," said Brig. Gen. Jim Isenhower, commander, 1MDTF.

Currently, the 915th CWB is aligned with Army Service Component Commanders at the Theater level and below, focused on supporting the MDTFs. While in competition phase, ECTs will assist in the targeting process, identifying potential enemy targets and presenting non-lethal effect options to neutralize the threat. Additionally, the teams will begin to characterize the enemy network through reconnaissance and surveillance in Cyberspace and Electromagnetic Spectrum surveys, not only providing visibility of the enemy disposition in the digital domain but identifying capabilities and offering counter-action options against those capabilities. During the penetrate phase, the ECTs will put this preparation into effect, neutralizing the enemy area denial capabilities and allowing maneuver units to seize the initiative through the "opening." The 915th CWB's unique close-access and proximal tactical capabilities will be critical in penetrating the enemy A2AD. Once "inside" the teams will begin the disintegrate period, combining close-area access with reach-back capabilities to deliver non-lethal cyber effects to the enemy's long-range assets. In support of the ground forces' rapid exploitation of the ground situation during the subsequent exploit phase, ECTs will provide isolation and command and control (C2) disruption through cyberspace, EW, and Information Advantage actions, further enabling the initiative. Once friendly forces achieve victory, forces will consolidate and enter the return to competition period. The ECTs will begin competition actions again on the next target or A2AD area of interest. Throughout each objective, the 915th CWB ECTs provides the Commander with critical maneuverability, valuable information, and non-lethal options to an otherwise hard-to-reach area.

Training for such a broad set of capabilities is challenging and requires a complex exercise to validate the processes needed to provide expeditionary CEMA. In December 2021, the 915th CWB will perform the first validation exercise of an ECT at Muscatatuck Urban Training Center (MUTC) in Indiana. The exercise is designed to stress ECT functions at each layer of support—strategic integration, targeting assistance, tactical maneuver, and OCO effects—throughout the course of five days. Extensive work on the Battalion METs, Mission Essential Task Lists (METLs), and a Cyber-Specific version of gunnery tables called Expeditionary CEMA Qualification Tables (ECQTs) was necessary to build the foundation for validating an ECT.

"We planned and executed our first internally resourced and controlled exercise at MUTC last October (2020)," said MAJ Byrne. "This was the first time the ECT was able to focus solely on its own METL and training objectives in a large-scale training event. The lessons learned over the last two years has molded the ECT into a capable team prepared for the next step to getting ECTs into real operations globally."

Whether it is creating virtual training environments, providing real-world and training communications networks, or using the included military intelligence personnel to provide accurate training scenarios, the experience and lessons learned from the CSCB pilot and the ECSD additions have all come to bear in creating an accurate and complex exercise.

The 915th CWB continues to evolve. Through exercises like MUTC, the ECTs train not only for the fight today, but stays poised for future MDO activities. As 915th CWB moves closer to becoming a fully-fledged, doctrine-backed, table of organizational equipment (TOE) unit, it will almost triple in size, and will have at least two validation exercises per year. Additionally, the process of deploying and supporting the fight will become streamlined, as the ECTs become regionally aligned and are integrated throughout each echelon. Lastly, the established 915th CWB's TOE and authorization documents—derived from the battalion's work developing the METL and force structure—will serve as a template for future units. In this way, the 915th CWB will always be remembered as a pioneer expeditionary CEMA.

The 915th Cyber Warfare Battalion is the Army's premier expeditionary CEMA force, poised to deliver effects anywhere in the world. Through the history of CSCB, ECSD and the 915th, cyber and EW Soldiers demonstrated exceptional ingenuity, persistence, and intelligence. These Soldiers are a remarkable testament to the adaptability of the Army.

"What our Soldiers will be called to do in the future will be different from what we are doing today, but one constant remains: 915th CWB Soldiers will continue to demonstrate the agility, innovation, and drive to determine what the Warfighter needs, integrate CEMA effects into tactical level operations, and win," said Lt. Col. Benjamin Klimkowski.

The 915th CWB, while still performing first-ever achievements, continues to build and prepare for the future of Army operations in the information dimension of the operating environment. – *Global Reach, Global Impact!*

From Front Desks to Frontlines: A Soldier's Account of the 915th Cyber Warfare Battalion

By Sgt. Mark G. Osterholt II, Bravo Company, 915th Cyber Warfare Battalion

Adaptability. Lt. Col. (LTC) William J. Cojocar, Ph.D., U.S. Army Retired, defined adaptability as "the ability to recognize changes in the environment, identify the critical elements of a new situation, and trigger changes to meet new requirements. Adaptability is an effective change in behavior in response to an altered situation."

IN 2014, THEN ARMY CHIEF OF STAFF GENERAL RAYMOND T. ODIERNO directed Army Cyber Command (ARCYBER) to assess the feasibility of integrating cyberspace operations into conventional maneuver at the tactical level. The resultant initiative sought to determine three things: whether cyberspace operations could be useful to brigade combat teams; what balance of capability and expertise would need to reside at that level for successful cyber integration; and how the force would need to change to adapt to warfare in the digital age. Throughout ARCYBER's efforts to integrate information advantage capabilities, 780th Soldiers have consistently innovated—developing the capabilities and the operator skills necessary to support the warfighter with Cyber Electromagnetic Activity (CEMA) effects.

Army senior leadership deliberated on the tactical cyber problem as early as 2012 and portions of 1st Information Operations (IO) Command recommended the integration of cyber teams into BCT training rotations as early as 2008. By 2014, the concept gained enough momentum to result in an Army Chief of Staff directed initiative. The 780th Military Intelligence Brigade (MI BDE) was tasked with answering the call. A handful of experienced cyberspace operations Soldiers and Civilians were selected to employ their skill set into the tactical environment which launched the Cyber Support to Corps and Below (CSCB) pilot program, later renamed the CEMA Support to CSCB. After many successful rotations in Combat Training Centers (CTCs), there was a higher demand for tactical cyber capabilities. On June 6, 2018, former Secretary of the Army, Honorable Mark T. Esper, directed ARCYBER to build the 915th Cyber Warfare Support Battalion (CWSB). On January 1, 2019, the Army approved the Table of Distribution and Allowances authorizing Soldiers to be officially signed to the 915th CWSB. On May 22, 2019, roughly five months later, the 915th CWSB activated under the command of LTC Matthew Davis. While building the battalion, the unit underwent a name change to the 915th Cyber Warfare Battalion (CWB). Today, the battalion has over 250 personnel, including three Companies, three Expeditionary Cyber Teams, and a fully functioning Battalion Staff element, which is a drastic change from the original CSCB Soldiers and Civilians that started the initiative.

Through the CSCB pilot program and the standup of the 915th CWB, evolution in both capabilities and work roles took place. When the CSCB pilot program began, the battalion was in the process of defining capabilities and training requirements. Every supported unit had different capabilities and different requirements making each CTC rotation unique and challenging. The evolution of capabilities and work roles occurred through experimentations, exercises, and formal Doctrine, Organization, Training, Materiel, Leadership and Education, Personnel, Facilities and Policy (DOTMLPF-P) assessments, leading to what it is today and enabling what it will become in the future.

The Evolution of Capabilities

At the beginning of the CSCB pilot program, the capabilities were antiquated, heavy, and in multiple large containers that were not man packable. To offer the tactical warfighter options to meet training objectives, it often took several vehicles to haul equipment which did not include the transport of Soldiers and their personal gear. This contributed to a series of questions – Is it realistic to transport this much equipment in a real-world situation? Can we project the capability requirements? Is there an easier and faster way to meet the intent? Maj. (MAJ) Sally White, the previous company commander and the first CSCB Officer-in-Charge, observed early that there was a lack of doctrine specific to expeditionary cyberspace operations, corresponding capabilities, knowledge of how an expeditionary cyber team would be constructed, and a lack of network infrastructure built into the CTCs.

"(The team would travel with over 40 pelican cases, weighing up to 99lbs, to various sites… Soldiers built mock networks to allow the testing of payloads and ensure the success of the exercise," said Master Sgt. (MSG) Alexander Simon, a former CSCB member. It

was evident that changes had to occur.

The 780th MI BDE began working on several activities simultaneously to provide the needed support to capabilities. Relationships were built across department of defense organizations, subject matter experts began pioneering commercial off the shelf (COTS) capabilities, and the requirements of each exercise were tailored to decrease the load of equipment often hand carried by CSCB members from site to site. Once given equipment and opportunity, the Soldiers and Civilians that supported the CSCB pilot program had the uncanny ability and skills to create long standing capabilities.

"We had a phenomenal group of Soldiers that would take an idea, plan for it, create the network, test the network, employ the necessary equipment, and reach the desired outcome," said MSG Simon.

A true testament to what the team within 780th MI BDE could do.

As the support CTC rotations continued, so did capability development. Lessons learned were shared with U.S. Army Training and Doctrine Command's DOTMLPF-P and the Cyber Center of Excellence to document not only the adjustments required to doctrine but also the development of future capabilities. Since the requirement was built and there was sufficient need for better, more robust capabilities, the Army Capability Manager Cyber (ACM-Cyber) has taken the role to assist in capability development for the now 915th CWB. ACM-Cyber continues to evolve capability management as the requirements adjust with the latest technology, target knowledge, and the tactical warfighter requirements.

The Evolution of the Expeditionary Cyber Operator Work Role

CSCB members, specifically the operators conducting tactical cyber operations, initially depended on resident knowledge, occupational skills, and certifications from their previous assignments to drive operations supporting the tactical warfighter. Gaps in both technical and physical capacity were identified early on when it was apparent that something had to be done to better prepare our Soldiers.

"I [did not] think for one minute that any 35Qs or early 17Cs ever thought they would be climbing mountains at NTC with a 50 pounds YETI battery along with all of our other normal kit. Much less sitting in the back of a Bradley or Stryker," remarked 1st Sgt. (1SG) Brian Fife, a previous CSCB founding member.

These tactical operators required specific skills ranging from technical knowledge and skills, physical prowess, and cyberspace operations planning, among a list of other critical skills.

"It was a steep learning curve if you are not used to managing sensitive equipment, logistics of personnel and equipment, care and feeding, constant S-3 (operations) and TOC (tactical operations center) briefings, integration with a CEMA cell, building the initial infrastructure you are targeting, developing new tool suites to make each successive home station training or Training Center iteration more challenging," added 1SG Fife.

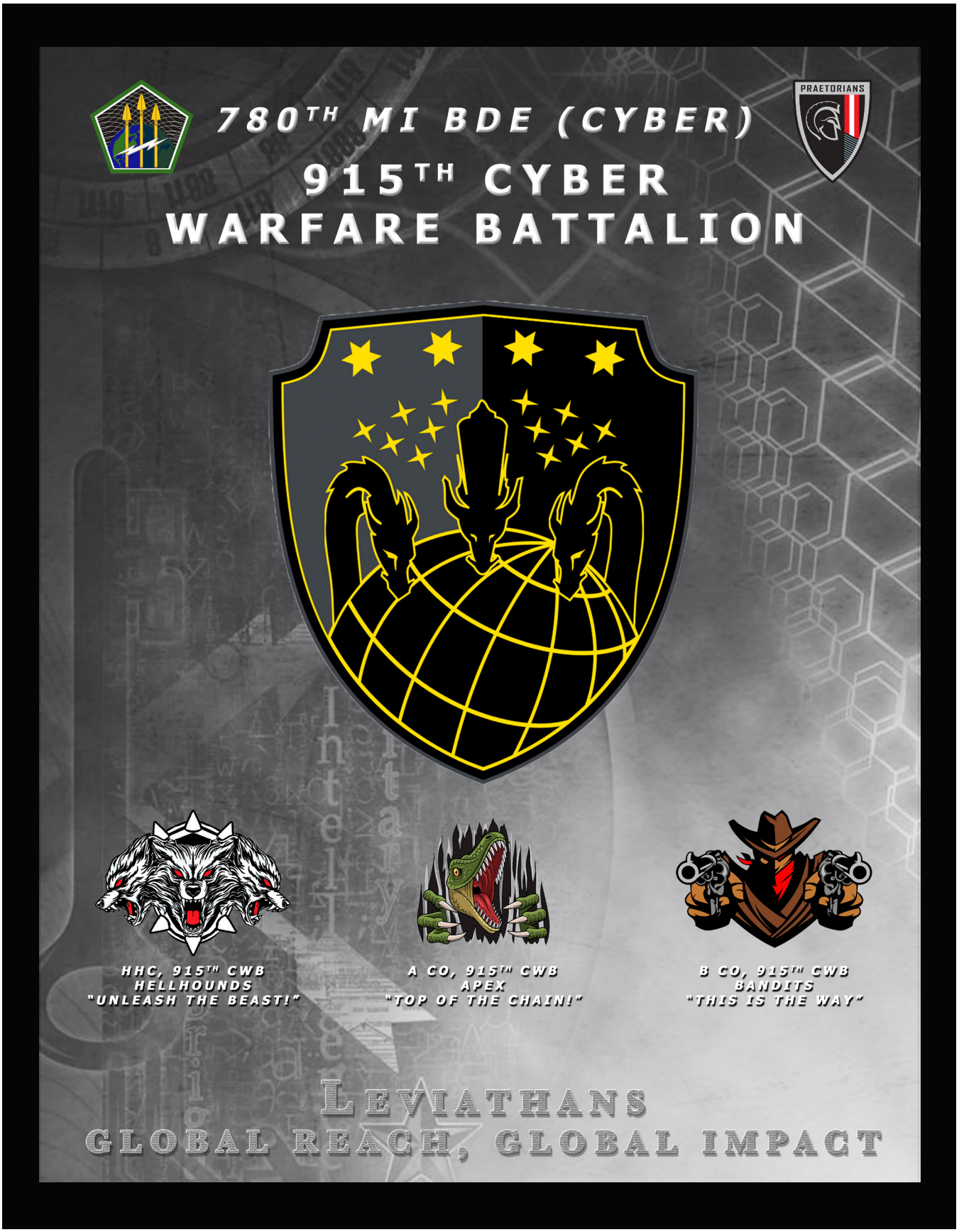
These activities led to the development of the Expeditionary Cyber Operator (ECO) work role for ARCYBER.

The ECO work role was first introduced in an ARCYBER work role seminar in 2016 where experts drafted the first basic level job qualification record (JQR). The initial intent was for ECOs to have the ability to be prepared for a wide range of activities, to include operating in urban areas, maneuvering with the tactical warfighter, vast targeting capacity against adversary communications, and the ability to integrate into non-conventional forces. Additionally, the initial JQR was built with a significant lack of conventional warfighting.

"When it comes to Expeditionary Cyber Operations, there has been a large gap between what Cyber does, how to request it, and how to implement it. With the many rotations at NTC, JRTC, [and] JMRC it has allowed for expeditionary cyber operators to brief leaders in a tactical unit on the implementation of cyber in the tactical arena," stated MSG Simon.

It was evident there was a wider breadth of knowledge, skills, and abilities (KSA) required, leading to the consistent development of the ECO work role.

Each year the basic, senior, and master ECO work role JQRs are reviewed by experts in the operational force. 1SG Fife shared every lesson learned from CTC rotations and unit engagements led to the evolution of the ECO and corresponding capabilities. The original intent for the ECO was primarily for cyberspace and military intelligence Soldiers. The evolution of the CSCB pilot and the establishment of the 915th CWB made evident the lack of electronic warfare (EW) knowledge and tasks. In 2021, experts across the field of cyberspace operations and EW collaborated to create a basic JQR to serve a multitude of operational KSAs to rectify this gap. The ECO JQR now focuses on both cyberspace and EW, expanding the KSAs to better support the aligned theater's requirements with the addition of electromagnetic spectrum activities. Each discipline will have specific tasks to accomplish in the JQR and will simultaneously share critical tasks that every ECO will be able to accomplish. This evolution of the ECO work role will continue to adapt every year as the environmental conditions and adversary capabilities evolve. – *Global Reach, Global Impact!*


780TH MI BDE (CYBER)
915TH CYBER WARFARE BATTALION
PRAETORIANS
HHC, 915TH CWB
HELLHOUNDS
"UNLEASH THE BEAST!"
A CO, 915TH CWB
APEX
"TOP OF THE CHAIN!"
B CO, 915TH CWB
BANDITS
"THIS IS THE WAY"
LEVIATHANS
GLOBAL REACH, GLOBAL IMPACT

780th Military Intelligence Brigade (Cyber)

(U.S. Army Photos)

780th Military Intelligence Brigade Operations

CEMA (Cyber Electromagnetic Activities) Support to Corps and Below (CSCB)

- Chief of Staff of the Army directed Cyber pilot (May 2014)
- Integration of service-retained cyber forces at the tactical level incorporating Cyber, Electronic Warfare and Information Operations

Support to Contingency Operations

- Maintains Title 10 platform to support Cyber Operations
- Supports cyber capabilities to disrupt extremist information dissemination
- Maintains an active cyber presence in support of the geographic combatant commands

Development Operations

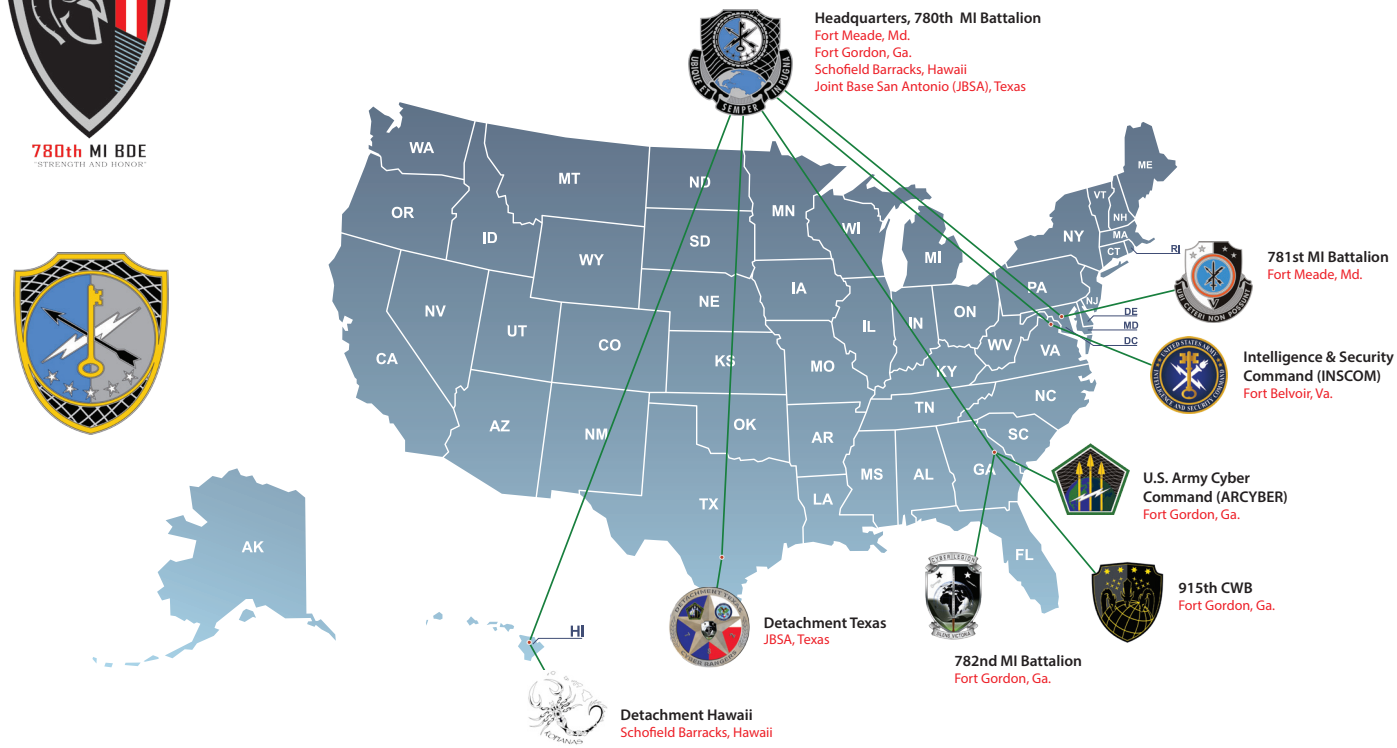
- Integrates Software/Hardware Development, Testing and Deployment to rapidly produc cyber tools in support of current operations
- Continuous Development Support Operations (incorporate operational feedback into capability development)
- Quick Reaction Capability Development (quick turnaround solutions to high priority missions)

Cyber Mission Force

- **National Mission Team/National Support Team** – Defend the Nation; conducts global cyberspace operations to deter, disrupt, and defeat adversary operations IOT defend US critical infrastructure and key resources
- **Combat Mission Team/ Combat Support Team** – Develop and employ offensive cyberspace capability to achieve or directly support CCMD objectives

780th Military Intelligence Brigade (Cyber)

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



780th MI Brigade Mission Statement:

Mission: The 780th Military Intelligence Brigade conducts cyberspace operations to deliver effects in support of Army and Joint requirements.

780th MI BDE Milestones: 2011-2021

Cyber Mission Force

- National Mission Team/National Support Team - Defend the Nation; conducts global cyberspace operations to deter, disrupt, and defeat adversary operations in order to defend US critical infrastructure and key resources.

- Combat Mission Team/Combat Support Team - Develop and employ offensive cyberspace capability to achieve or directly support Combatant Command objectives.

- CPT/Incident Response - Cyber Protection Teams remediate foreign threats local and foreign networks; currently supporting NSA capability remediation efforts

780th Military Intelligence Brigade (Cyber) Milestones from December 1, 2011, to December 1, 2021

- Led the Nation's effort to complete the build of the Army's Offensive Cyber Mission Force
  - » Brought all 21 of the brigade's cyber mission teams to full operational capability – the first element of any of the Services to meet this milestone achievement
- Maintained and fostered command relationships with U.S. Army Cyber Command, U.S. Army Intelligence and Security Command, the Cyber National Mission Force Headquarters, and multiple Joint Forces Headquarters – Cyber across multiple Services and Joint elements
  - » Executed operations with tactical, operational, and strategic impacts
  - » Supported four different Combatant Commands
  - » Supported garrison requirements across four military installations
- Established and expanded multiple Joint Mission Operation Centers from which offensive cyberspace operations are conducted by not only the brigade, but sister-Service cyber teams as well
  - » These locations have increased the capacity to conduct operations by teams of the brigade and across the Cyber Mission Force (CMF)
  - » In June 2016, the brigade conducted one to two operations per month. As a result of the expansion there are multiple operations that occur 24/7
- Integrated the largest Army National Guard (ARNG) mobilization (Task Force Echo) ever for USCYBERCOM
  - » Seamless changeover between two ARNG formations whereby one cyber battalion transitioned with another to continue the Task Force Echo cyberspace mission

» Currently on the sixth iteration of Task Force Echo

- Established Cyber Solutions Development (CSD) Detachment and consolidated developers
  - » Formed to consolidate previously dispersed cyberspace tool developers, and focus efforts to build solutions for both the CMF, and Army-specific cyberspace needs
  - » There is now a CSD-M (Maryland); CSD-G (Georgia); CSD-TX (Texas); CSD-T (Tactical); and CSD-H (Hawaii)
- Trained more than 200 Developers and initiated a Job Qualification Requirement (JQR) process to test and advance capabilities
- Informed the Fiscal Year 2019-2021 Cyber Warfare Battalion build through Cyber/Electro-Magnetic Activities (CEMA) Support to Corps and Below (CSCB) efforts
  - » Executed support at four National Training Center rotations, one Joint Readiness Training Center rotation, and one Joint Military Readiness Center rotation providing fully integrated offensive elements to expeditionary CEMA teams (ECTs) embedded with the rotational unit during both home-station training and during the training rotation
  - » During Defender Pacific and Forager 21, integrated with the Multi-Domain Task Force (MDTF) and the Multi-Domain Effects Battalion (MDEB) to validate MDTF objectives supporting future multi-domain concepts of employment
  - » Supported two Warfighter Exercises (WFXs) to inform CEMA planning and integration concepts at the Corps and Division level
  - » Executed the first annual training exercise for the 915th CWB at Muscatatuck, IN in 2020 which provided the framework for future annual assessment events for ECTs
- Evolved Assignment Incentive Pay (AIP) / Special Duty Assignment Pay (SDAP) to recognize and reward our talented population
- Kept the Army's leadership informed of our progress toward manning and training our cyberspace operations professionals to execute missions globally
  - » Articulated a readiness model for offensive cyberspace operations forces
  - » Provided the clear vision that forces our Army to look at our offensive cyber teams as they would any other maneuver force
  - » Established a standard of cyber firing crews with minimum manning and training requirements
  - » Clearly and accurately communicated the level of readiness defined by the number of crews trained and available to execute offensive cyberspace operations ■

(Photo by Capt. Adam Schinder, 782nd MI BN)

Task Force Echo – America's Citizen Soldiers

By Lt. Col. David Garner, commander, 123rd Cyber Protection Battalion and Task Force Echo V, and Maj. Nicholas Allen, S-3 (Operations), 123rd CPB, TFE V

IN 2008, THE 123RD DATA PROCESSING UNIT (DPU), a unique formation that was established in 1975 to process pay for the entire National Guard using mainframes and punch cards, began sending Soldiers to conduct a mission at Fort Meade known as the Kodiak Cyber Operations Team (KCOT). The DPU was also tasked with cyber incident response within the state of Virginia and was a frequent attendee of national-level cyber exercises. In 2017, a critical need for support was identified by U.S. Cyber Command (USCYBERCOM), and the DPU became the first unit to be mobilized as part of a new mission named Task Force Echo (TFE).

During that first TFE mobilization, the Virginia Army National Guard (ARNG) underwent a major change in force structure. The 91st Troop Command was reflagged to become the 91st Cyber Brigade, and the 123rd DPU was split into the 123rd and 124th Cyber Protection Battalions (CPB), with the 91st growing in size and capability over the next five years. Today the 91st Cyber Brigade consists of five battalions, and has units in more than 30 states and territories.

Task Force Echo is an ARNG Task Force mobilized annually to engineer, install, operate, maintain, and defend critical network infrastructure and conduct cyberspace operations in support of USCYBERCOM and the Cyber National Mission Force. TFE also provides oversight and support to the Cyber Warfare Company (CWC) mission conducted in support of Joint Force Headquarters-Cyber (Army), a mission that has grown in size and scope from the historic KCOT mission.

TFE is aligned under and operationally controlled the 780th Military Intelligence Brigade (Cyber) and is administratively controlled by Army Cyber Command (ARCYBER). The mission is sourced from the 91st Cyber Brigade (Va.) and its five subordinate CPBs and consists of 150 ARNG Citizen Soldiers. TFE Rotations last for a total of 445 days, including 45 days of Title 32 work-role training that is contracted by ARCYBER. Each of TFE's more than 60 work roles have a unique training pipeline to prepare them for their mission requirements. Task Force Echo is currently in the fifth iteration of the mission, and it is anticipated to continue for an additional two rotations (to TFE VII).

TFE relies heavily on the diverse technical backgrounds endemic to the Soldiers of the National Guard. They bring extensive experience to the mission that can only be gained by working in defensive cyberspace, network infrastructure, computer programming, and other information technology positions throughout the private sector as well as the completion of the extensive training required to be a cyber warrior.

According to the 780th MI Brigade commander, Col. Matthew Lennox, "The annual TFE rotation allows for highly technical group of Soldiers to come in with a fresh set of eyes, thus leading to provide new ideas and innovation, and over the years have made continuous improvements to the infrastructure, security, and processes which adds great value to the 780th MI BDE and the JMOC (Joint Mission Operations Center)." Many of the innovative ideas and improvements have been adopted as best business practices in all JMOCs, and TFE has many products that feed and display mission data to the JMOC-Enterprise as well as ARCYBER and USCYBERCOM.

TFE provides an opportunity for National Guard Soldiers to obtain the education and experience they need to get the Cyber Protection Team(s) to IOC (initial operating capacity) and FOC (fully operational capacity). Upon return to home station, Soldiers will possess an increased skill set and with hands-on experience. This provides the National Guard increased capability supporting federal missions and provides Governors and Adjutants General with additional capabilities to support state missions. ■

Task Force Echo (TFE) Map

Task Force Echo I
123rd Cyber Protection Battalion
The 123rd Cyber Protection Battalion was comprised of Army National Guard (ARNG) Soldiers who hailed from California, Georgia, Indiana, Ohio, Michigan, Utah, and Virginia

Task Force Echo II
125th Cyber Protection Battalion
The 125th Cyber Protection Battalion was comprised of ARNG Soldiers who hailed from Louisiana, Mississippi, New Jersey, New York, South Carolina, Texas, and Utah

Task Force Echo III
126th Cyber Protection Battalion
The 126th Cyber Protection Battalion was comprised of ARNG Soldiers who hailed from Alabama, Colorado, Connecticut, Kentucky, Maine, Massachusetts, New Hampshire, North Dakota, South Dakota, Tennessee, Utah, and Vermont

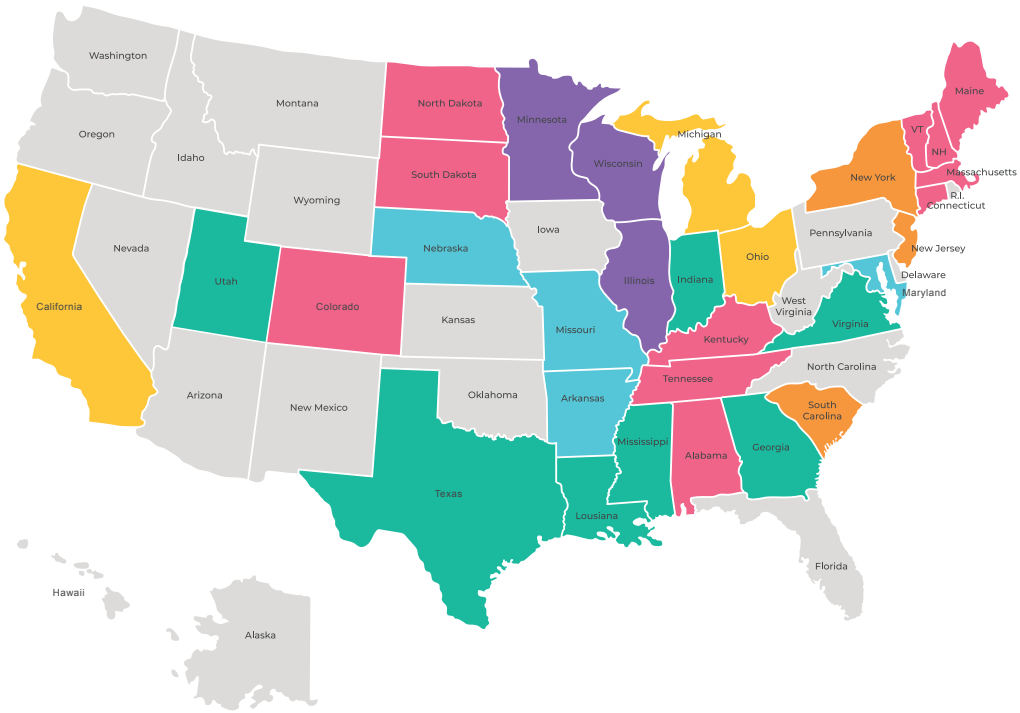
Task Force Echo IV
124th Cyber Protection Battalion
The 124th Cyber Protection Battalion was comprised of ARNG Soldiers who hailed from Arkansas, Maryland, Missouri, Nebraska, Virginia, and Utah

Task Force Echo V
123rd Cyber Protection Battalion
123rd Cyber Protection Battalion, was comprised of ARNG Soldiers who rhailed from Illinois, Minnesota, Virginia, and Wisconsin

Task Force Echo VI
127th Cyber Protection Battalion
127th Protection Battalion, is comprised of ARNG Soldiers who hail from Georgia, Indiana, Louisiana, Mississippi, and Texas

Multiple TFE Supporting States

Non-TFE Supporting States



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

HHC, 780th MI BDE Byte Article – "Hastati Through the Years"

By Capt. Lauren Feifer, commander, Headquarters and Headquarters Company, 780th Military Intelligence Brigade (Cyber)

"THE HEADQUARTERS AND HEADQUARTERS COMPANY (HHC) is doctrinally designed to sustain the mission of the brigade and is built on a foundation of interdisciplinary support elements. When the 780th Military Intelligence Brigade (Cyber) was formally activated in 2011, an undeniable element to facilitate the operational environment was the HHC.

Within the Brigade S1 (personnel) team, Sgt. 1st Class Kimberly McKenzie shared the following on the importance of the overall role of an HHC. "An HHC is a key element because its sole purpose is to provide communication, supply, and administration support to subordinate units. With the HHC support it allows the subordinates to focus on the accomplishment of the Army mission. HHC's role in the fight can be directed in several critical roles to give its maximum tactical advantage and strengthen a unit's value. HHC is often charged with leading several mission essential task list training pathways and ensuring combat readiness. The HHC is deliberately manned and equipped to best support the unit's mission, the HHC is often an untapped asset for key supporting roles."

A particularly unique aspect of the 780th MI BDE (Cyber) HHC is the composition of Soldiers and Civilians. While many traditional Army units have a majority strength of Soldiers, Hastati Company is equally comprised of Soldiers and Civilians, creating a diverse and distinctive culture throughout the years. With more than 160 personnel, the company has traditionally been committed to ensuring all personnel are welcome, included, and developed to perform at their best. Many of the Company's Civilians have prior military service, enabling them to better mentor new Soldiers within the unit while sharing unique lessons learned in an exponentially distinctive environment.

Coming from a Team in Texas, Sgt. Anthony Shingara shares how operating in this different, yet rewarding environment has fostered his own personal and professional growth. "Coming from NSA Texas where we had a similar team make up of Military and Civilian personnel, coming here wasn't that hard of a transition in the workplace to me. However, I learned very quickly from my first assignment here at Brigade that if you do not take the time to reach out and build those important inter-organizational relationships you are not going to make it far, both in your work role and as a member of the team. I was a bit of a shut in when I first arrived and as a result, I never really got a chance due to my own fault to develop those professional relationships here. When I transitioned over to the Brigade S3 (operations) Training shop I made sure to not squander the opportunity to make those relationships. The Brigade S3 Training shop has many personalities and a plethora of experience from both past and current military members and from civilians who have been with the Brigade for a while. I am learning new things every day from them and its only making me a better training NCO and a Soldier all together. I'm truly blessed to be able to work with the amazing men and women who make up the Brigade S3 Training shop, and I'm grateful for all the knowledge they have instilled in me."

While the foundational values of the organization have remained largely unchanged, HHC Brigade has modified the unit's emblem since its initial inception. Upon the brigade's activation in 2011, the company initially stood up as "The Honeybadgers". Carrying this heraldry for almost seven years, the company rebranded as "Hastati" in 2018 bearing the motto "Facta, Non Verba", translating to "Actions, Not Words". The Company Command Team spearheading this initiative promoted a professional and honest motto to encourage an atmosphere of excellence.

Hastati, meaning "spearman", were Soldiers that represented the first line of defense for the Roman Republic. Formed from diverse sects of people, the Hastati incorporated a variety of weapons within their defense structure. Like these ancient warriors, the Hastati Headquarters and Headquarters Company is built and thrives on the unique and varied skills of each staff section. Whether it is the mission of the special staff, S1 (personnel) through S6 (IT) sections, or the Orderly Room, each element is essential to effectively supporting the operational teams within the brigade.

As the mission of the 780th MI Brigade (Cyber) continues to expand and develop, so will the Soldiers, Civilians, and contractors that comprise Hastati Company. If the COVID-19 pandemic has taught leaders within the organization one crucial lesson, it is that all Soldiers, Civilians, and contractors within the Hastati Company will continue to service the mission no matter the obstacle. Regardless of the challenges the next ten years will bring (hopefully one day in a newly refurbished headquarters building), HHC Brigade is prepared and will continue to adapt to serve all personnel within the Praetorian Family. ■

FORT GEORGE G. MEADE, Md. – The company's guidon was uncased and unfurled by Lt. Col. Eric Remoy, deputy commander, 780th MI Brigade, and Command Sgt. Maj. Lawrence Hoke, 780th MI Brigade.

Cyberspace Beginnings: Detachment Meade

An excerpt from Maj. Sarah "Sally" White Ph.D. dissertation (Harvard, 2019)

THE INTELLIGENCE COMMUNITY'S EXPLORATION of cyberspace operations emerged in response to the growing importance of digital communications to signals intelligence collection. In the summer of 1995, the 704th Military Intelligence Brigade — the Army's signals intelligence brigade within INSCOM – devoted a small element of twenty-five personnel to support information warfare combat development.[1] The lack of an unclassified doctrine for computer network operations hindered the element's ability to inspire a larger conversation.[2] This effort expanded in June of 1998, when the 704th was tasked to develop a computer network operations force for the Army.[3] In response, B Company of the brigade's 742nd Military Intelligence Battalion dedicated a small platoon of soldiers to CNO.[4]

742nd MI BN crest

In June of 2000, this small effort grew into Detachment Meade, an outfit of approximately three dozen soldiers that was established to sustain the growing need for an Army computer network operations force.[5] Detachment Meade maintained a close relationship with LIWA and later 1st IO Command in two ways: by providing capabilities for LIWA to integrate into its IO planning, and by leveraging LIWA's special technical operations (STO) accesses in support of CNO missions.[6] By the mid-2000s, aided by a special recruitment and assessment program to identify enlisted soldiers, the detachment had grown into a highly specialized and highly skilled force of just under 200 personnel.[7] However, the detachment faced a number of challenges that impeded its ability to have a far-reaching impact on Army cyberspace development.

First, the organization was small and shrouded in secrecy, a by-product of its origins in the compartmentalized world of signals intelligence.[8] The Army Cryptologic Office, operating under the belief that cyber was simply SIGINT with a different name, continued to enforce heavy classification schemes and limited experimental authority even as the Detachment's growing cohort of CNO practitioners began to lobby otherwise.[9] Efforts to increase awareness beyond the SIGINT community were complicated by the lack of any unclassified doctrine on computer network operations, which did not arrive until the 2003 edition of FM 3-13.[10]

Second, the lack of a dedicated computer network operations career field meant that the detachment had a hard time finding qualified soldiers to fill its ranks and a hard time training them once they arrived. Absent a formal training progression, consistent course availability, or an adequate training budget, Det Meade soldiers had to rely heavily on individual self-study to rectify gaps in their technical knowledge.[11] The lack of a dedicated career field also caused retention challenges: because detachment soldiers were managed by their traditional intelligence occupation specialties, the soldiers faced the constant threat of being moved into a more conventional assignment by the Army personnel system. This threat was all the more pressing due to the high demand for SIGINT support to the wars in Iraq and Afghanistan.[12]

The 704th responded to these retention challenges by relying on a special management program to temporarily protect soldiers from reassignment. However, this program complicated the unit's efforts to interface with the regular Army.[13] When coupled with the fact that most of the Army's CNO capabilities fell under compartmentalized special access programs, Det Meade's special management program meant that deployed units would often find it easier to ignore the small CNO teams they received rather than find a way to integrate them into their operations.[14] In part to rectify this dysfunction, a number of the detachment's early key leaders tried to push for better talent management and a more normalized force structure. This effort began in 2003 and culminated with the declaration, several years later, of the D6 ASI for enlisted personnel and the E4 ASI to identify officer CNO planners.[15] The ASI designation enhanced the Army's ability to determine which of its soldiers had cyber skills, but it did not guarantee that those soldiers would serve in cyber assignments. As such, it was only a temporary solution to the detachment's personal challenges.

Third, Detachment Meade lacked consistent support from its higher leadership. Whereas one brigade command team might see potential value in the unit, the next would think it useless and try to shut it down.[16] The unit struggled to maintain access to resources and often operated without much guidance or sense of direction. In the absence of a coherent vision for what Army cyber should be, and without much capability to drive the creation of such a vision, the detachment invested heavily in National Security Agency relationships to keep their cyber-savvy soldiers gainfully employed.[17] While this strategy of inter-agency investment helped cultivate a deep bench of skill, it also hindered the detachment's ability to conceptually innovate and exacerbated the ongoing debate over whether cyber was

SIGINT or something new.

The combination of inconsistent chain of command support and a lack of clear guidance on the detachment's purpose resulted in the SIGINT community pursuing an ad hoc approach to computer network operations from 1998-2006.[18] The early computer network attack capabilities and concepts that emerged from SIGINT organizations were thus largely indistinguishable from traditional methods of active SIGINT or electronic warfare.[19] As such, they were expected to deliver in the same way that SIGINT delivered during the heyday of the global war on terror: by providing an increased understanding of how threat actors were using the internet to perpetrate violence.[20]

The Growth of a Cyber Battalion and Brigade

These years of languid growth for the intelligence community's cyberspace operations began to shift after 2005. Two things happened that year that influenced the growth of computer network operations: first, STRATCOM stood up JFCC-NW and tasked the services to provide support, which provided a consistent demand signal for cyberspace operations; second, Lieutenant General Keith Alexander was appointed the director of the National Security Agency. In 2007, Detachment Meade was renamed the Army Network Warfare Detachment.[21] In 2008, this detachment became part of the Computer Network Operations Task Force. On 2 June 2008, the CNO-TF became the Army Network Warfare Battalion (Provisional), a 182 person organization with the mission "to conduct offensive computer network operations in support of strategic, operational, and tactical requirements"[22] at the national, joint, and Army levels.[23] In October of 2009, this unit was redesignated as the 744th Military Intelligence Battalion, a 245 person organization that conducted tool development, expeditionary, and remote cyberspace operations for the Army.[24] In December 2011, the 780th Military Intelligence Brigade (Cyber) was activated under INSCOM, marking the end of a five-year period of rapid organizational growth.[25]

References:

1 CW5 Al Monteiro, interview with the author, 7 December 2018. CW5 Monteiro was intimately involved with Det Meade from 1999 onward and has been called "the father of Army cyber" by many of his contemporaries. Estimates put this element at roughly 25 personnel.

2 Monteiro, interview.

3 "History, 780th Military Intelligence Brigade," INSCOM.mil, accessed Sep 9, 2018, https://www.inscom.army.mil/MSC/780MIB/history.html.

4 Monteiro, interview.

5 "History," 780th Military Intelligence Brigade. Monteiro placed the initial estimate between 36 and 39 personnel, only around half of whom had the necessary skill set to engage in the detachment's mission.

6 Monteiro, interview.

7 Monteiro, interview.

8 One 742nd BN CDR who took command in mid-2003 didn't even know about Det Meade until a month into her command. In this, Det Meade was as much of an unknown quantity to its own parent organization as it was to the larger Army. (Lisa Bennett, telephonic interview with the author, Oct 23, 2018).

9 On ACO, see "Army Cryptologic Operations," U.S. INSCOM website, last updated May 2, 2019, https://www.inscom.army.mil/MSC/ACO.aspx, and Headquarters, Department of the Army, Field Manual 2-0, Intelligence (Washington D.C.: Headquarters, Department of the Army, March 2010), section 12-8. The ACO perspective on this subject came from McNeill, William and Wetzel, Thomas, interview with the author, Fort Meade, M.D., Sep 24, 2018. The cyber perspective came from Minnick, interview, and George G. Franz, email correspondence with the author, Aug 12, 2018.

10 Monteiro, interview.

11 Homer Minnick, interview with the author, 23 July 2018. Minnick was one of the original members of Det Meade.

12 Lisa Bennett, interview with the author, 23 October 2008. COL(R) Bennet commanded the 742nd MI BN from 2003-2005.

13 Monterio, Bennett, interviews.

14 Bennett, interview. On SAPS, Monteiro, interview. Partially as a result of these difficulties in supporting the conventional force, Det Meade shifted its focus to the special operations community in the mid-2000s.

15 Lisa Bennett began the effort to establish a CNO ASI but ran into resistance from her brigade commander. The D6 ASI specifically referred to soldiers who had completed the Basic Digital Network Analyst (BDNA) course. Memorandum from GEN Petraeus, 26 July 2008, discusses need for a CNO planner ASI in addition to the D6. Technically, the E4 ASI requires a minimum of 12 months of service in the Cyber Mission Force.

16 For example, Lisa Bennett's efforts to develop an ASI and bring the unit into the open were followed by a commander who wanted to shut the unit down and repurpose its soldiers for SIGINT support to the GWOT.

17 Minnick, interview.

18 Minnick, interview. ANWB provided briefings or hosted visits for more than 50 distinguished visitors in FY09, most of whom were members of the intelligence community itself. This data point suggests that, even as late as 2009, the Army's CNO community continued to struggle to sell itself to its own parent intelligence organizations. "744th Military Intelligence Battalion (ANWB) Historical Summary FY09," 11.

19 Minnick, Monteiro, Easterly, interviews.

20 LTC(R) Jen Easterly, telephonic interview with the author, Nov 6, 2018.

21 "History," 780th Military Intelligence Brigade.

22 Mission from COL Douglas A. Wild, Permanent Orders 170-01, "Network Warfare Battalion (Provisional) (W00150), Fort George G. Meade, Maryland 20755, 18 June 2008 [FOIA 142]. Personnel strength from Jay C. Waters, Permanent Orders 246-01, 3 September 2009 [FOIA 409].

23 "Army Network Warfare Battalion (ANWB) Officially Activated," no date [FOIA p. 440]

24 "744th MI Bn (ANWB)" [FOIA p. 404], "Headquarters and Headquarters Company" [FOIA 405], "Alpha Company" and "Bravo Company" [FOIA 407-408]

25 "Army Cyber Chronology," no date, received from Scott Anderson, Army cyber historian, via email. The brigade was originally going to be called the 1st Army Cyber Brigade, but then fell into line with the INSCOM unit naming series. All INSCOM units are intelligence units in the 100/500/700 series range. Since the 700 series are strategic assets, and INSCOM believed the cyber brigade would be a strategic asset, it was decided to call it the 780th MI Brigade. (Thompkins, interview).

780th Military Intelligence Brigade (Cyber)

History

The 780th Military Intelligence (MI) Brigade (Cyber) was activated on Oct. 1, 2011, as a Major Subordinate Command under the U.S. Army Intelligence & Security Command (INSCOM), while also serving under the operational control of U.S. Army Cyber Command (ARCYBER). The 780th MI Brigade is the only offensive cyberspace operations brigade in the U.S. Army, and we actively fight alongside our Joint partners to achieve U.S. supremacy in an increasingly contested cyberspace and electromagnetic spectrum.

The history of the 780th MI Brigade dates back to 1995 when the Technical Analysis Activity (TAA) was created within the Army Technical Control and Analysis Element (ATCAE). In the ensuing years, the 704th MI Brigade was tasked to develop a computer network operations force for the Army and in June 1998, B Company, 742nd MI Battalion evolved out of the TAA and answered the call.

In June 2000, Detachment Meade, 742nd MI Battalion was established to sustain the growing need for an Army computer network operations force. Detachment Meade was re-designated as the Army Network Warfare Detachment in 2007 and in June 2008 the Task Force was again re-designated as the Army Network Warfare Battalion (Provisional). The following year the battalion moved beyond its provisional status and was designated the 744th MI Battalion (Army Network Warfare Battalion).

In December 2010, the Army approved the establishment of a cyberspace operations brigade, and on October 1, 2011, the 780th MI Brigade was organized. Subsequently, the 744th MI Battalion was re-designated as the 781st MI Battalion and re-organized under the new brigade. The 780th MI Brigade officially unfurled its colors for the first time during a ceremony at Fort. Meade, Maryland on December 1, 2011.

The brigade began building a second battalion headquartered at Fort Gordon, Georgia in 2011 culminating with the stand-up and designation of the 782nd MI Battalion on June 7, 2013. Detachments Texas and Hawaii were organized as part of the 782nd MI Battalion in 2013 and 2014 respectively giving the brigade a footprint in four states in support of multiple operational headquarters.

In July 2017, the 780th MI Brigade established the Cyber Solutions Development Detachment. The Detachment takes its place as the newest addition to the brigade focused on innovative solutions across the spectrum of cyberspace operations. Subsequently, there are now CSD detachments at both Forts Meade and Gordon.

Since August 15, 2017, U.S. Army National Guard Soldiers have been mobilized and assigned to Task Force Echo, an organization conducting cyberspace operations in support of U.S. Cyber Command and the Cyber National Mission Force. The Task Force is aligned under the 780th MI Brigade, which falls under the operational control of U.S. Army Cyber Command.

On June 6, 2018, the Department of the Army directed U.S. Army Cyber Command to activate the 915th Cyber Warfare Battalion (915 CWB). Subsequently, ARCYBER directed the 780 MI Brigade assume Command Authority and administrative control of the 915th CWB. The 915 CWB is the first scalable organic expeditionary capability to meet the Army's current and projected tactical cyberspace requirements, including the integration of cyber and electronic warfare.

In less than ten years, the 780th MI Brigade's mission has increased in scope, scale, and complexity. The unit is known among ARCYBER, U.S. Cyber Command, and senior Army leaders as a world class cyberspace operations force capable of providing a ready force, developing capabilities required to meet expanding requirements, and delivering effects at the time and place of the operational commander's choosing.

FORT GEORGE G. MEADE, Md. – 780th MI Brigade first Anniversary.

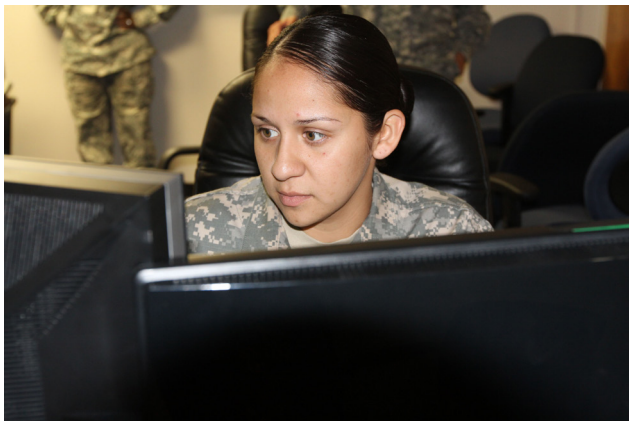
FORT GEORGE G. MEADE, Md. – The 780th MI Brigade (Cyber) holds its first official brigade run on December 2, 2011.

FORT GEORGE G. MEADE, Md. – 780th MI Brigade first promotion board.

FORT GEORGE G. MEADE, Md. – Spc. John Gonzalez, information management, 780th MI Brigade, tests the communication lines for connectivity to the Defense Information Systems Agency cloud.

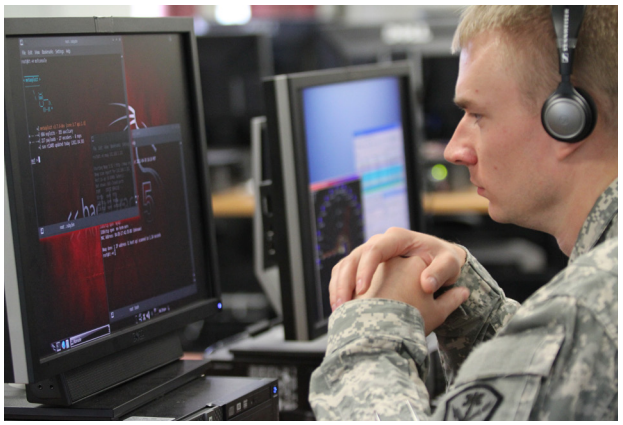
PENTAGON, DC – Soldiers of the 781st MI Battalion recite the Army reenlistment oath during a formal ceremony at the Pentagon.

FORT GEORGE G. MEADE, Md. – The 780 MI Brigade's first change of command between the outgoing commander, Col. (COL) Jonathan E. Sweet, and then-COL Jennifer G. Buckner was hosted by Lt. Gen. Stephen G. Fogarty, then the commander of U.S. Intelligence and Security Command and currently the commanding general of U.S. Army Cyber Command.



FORT GEORGE G. MEADE, Md. – Command Sgt. Maj. William Rinehart administered the Oath of the Noncommissioned Officer to the latest inductees of the 781st MI Battalion held March 8, 2013.


AKERS
U.S. ARMY




U.S.ARMY
15.0 V

New Cyber Brigade Activates

By Tina Miles, Public Affairs Officer, 780th Military Intelligence Brigade

*Note: This story was originally released December 1, 2011

FORT MEADE, Md. – Network warfare, cyber security and the illegal release and posting of classified information on the internet are all hot topics in recent news headlines – topics which the government, and more importantly its military, take very serious.

The nature of that seriousness is evident with the Army's recent activation of its first computer network operations brigade.

With an urgent insistence and tremendous help from the National Security Agency, Department of Defense and U.S. Cyber Command, Army and Congressional staff, the U.S. Army Intelligence and Security Command created the 780th Military Intelligence Brigade to support U.S. and Army Cyber Commands with their missions to provide a proactive cyber defense.

In an event that marked the culmination of years of preparation, the colors of the 780th MI Brigade were unfurled for the first time during an activation ceremony at NSA's Friedman Auditorium, here, Dec. 1.

"While normally it is enough to gather in time-honored tradition to pass unit colors to mark the transition of commanders and continuity of mission, on really rare occasions like today we have the opportunity to activate a new unit – hand-picked, specifically recruited and purpose built, which has and will continue to contribute to a complex fight against those who present a clear and present danger to our nation's security, while providing new and breathtaking capabilities to our Army's already impressive portfolio of warfighting capabilities," said Maj. Gen. Mary A. Legere, INSCOM commanding general.

Though fully preoccupied with two wars in the Middle East, engaged in other operations globally and confronted by resource constraints that might have been an excuse for inaction, the Army empowered INSCOM to once again build a unit in response to a specific threat – providing it with the mandate, mission and resources to form this brigade.

In December 2010, the Army approved the establishment of an Army Cyber Brigade and designated the 780th MI Brigade to fulfill this mission with an effective date of Oct. 1, 2011.

"'Never rely too heavily on intuition. It will never be a good substitute for good intelligence," said Legere, quoting a phrase from Gen. Omar Bradley. "It is his spirit, and in response to a sense of foreboding, that our Army has had the wisdom to resource and create the 780th."

The ceremony also marked the assumption of command for Col. Jonathan E. Sweet, as he accepted the colors from Legere.

"Aug. 19th, 1942, Maj. Gen. Lee, commander of the newly formed 101st Airborne Division, told his Soldiers assembled at Camp Claiborne, La., that 'the 101st has no history, but it has a rendezvous with destiny,'" said Sweet. "These men were the infantry's best-of-the-best. They were selected, trained and deployed to counter an adversary that threatened our country during the Second World War."

Sweet compared his new brigade to a more seasoned one.

"Like the 101st, the 780th MI Brigade has no history, and was formed to counter an adversary operating in a different domain – a highly technical, manmade domain called cyberspace," Sweet added.

While recognizing numerous individuals responsible for the creation of the brigade, and those who assisted his career accomplishments, Sweet said it is an honor to have the opportunity to return to Fort Meade and join Command Sgt. Maj. Lawrence Hoke, 780th MI Brigade command sergeant major, to activate, command, and operationalize this incredibly special brigade.

"The first 26 miles of this marathon began in October 2002, with the activation of Detachment Meade. Since then it's evolved and expanded into the Army's Network Warfare Battalion, assembled a headquarters company and staff, and today the 780th MI Brigade," said Sweet. "As we cross this finish line and take a moment to enjoy the accomplishment, we're reminded that it's merely a transition point, providing us enough time to catch our breath and get ready to step out across the start line for the next phase of what is actually a triathlon."

The brigade's 781st MI Battalion and Headquarters and Headquarters Company, at Fort Meade, and the 782nd MI Battalion, located at Fort Gordon, Ga., will collectively enable the unit's mission to conduct signals intelligence, computer network operations, and when directed, offensive operations, in support of DoD, Army and interagency operations worldwide, while denying the same to its adversaries.

"This [activation] is a tribute to the belief in the notion that our nation requires assured freedom of maneuver in cyberspace in this era of persistent conflict and the advent of the increasingly more sophisticated threats to our security," Legere added.

Legere added that the Army's newest brigade is fully prepared to assist Gen. Martin E. Dempsey, chairman of the Joint Chiefs of Staff, and Gen. Raymond T. Odierno, chief of staff of the Army, as they forge ahead in promoting cyber defense and full spectrum Cyber Ops as one of their top priorities, and in helping Gen. Keith B. Alexander, commander of USCYBERCOM and director of the NSA, as he continues to educate, implore and challenge our nation's leadership to take decisive action to develop and expand this kind of capability that is now so critical to our nation's security.

"The challenge to our nation in this domain is upon us. You see this every day. The future danger that you envisioned has arrived," said Legere. "And the time for the men and women of the 780th to take your place in the Army's long gray operational line as a fully resourced operational unit ready for action is now."

FORT GEORGE G. MEADE, Md. – Col. Jonathan Sweet, commander, 780th MI Brigade (Cyber), unfurls the brigade colors for the first time at an activation ceremony held December 1, 2011, on the NSA complex.

FORT GEORGE G. MEADE, Md. – 780th MI Brigade (Cyber) first staff.

Recognizing the Cyber Challenge

By Tina Miles, Public Affairs Officer, 780th Military Intelligence Brigade

*Note: This story was originally released May 23, 2012

FORT MEADE, Md. – The next phase of the 780th Military Intelligence Brigade's history began Tuesday as officials broke ground for the newly formed brigade's headquarters facility during a ceremony here.

Members from the U.S. Army Intelligence and Security Command, 780th MI Brigade, Army Corps of Engineers, Baltimore District and Fort Meade Garrison took part in the momentous occasion further enabling the Army's goal of providing the force with the best in cyber security.

"Today marks the next step in our Brigade's path to become fully operational," said Col. Jonathan E. Sweet, commander, 780th Military Intelligence Brigade. "This 46,000 square foot facility will serve as the brigade's headquarters, operations center and training facility and allow us to accomplish our mission – to provide proactive cyber defense and to conduct full spectrum cyber operations for our nation."

During his remarks, Brig. Gen. Robert L. Walter, Jr., INSCOM deputy commanding general said Army's technical advancements in detection and attribution shed light on malicious activity, but cyber intruders continue to explore new means to circumvent defensive measures.

"Data collection, processing, storage and transmission capabilities are increasing exponentially...the impact of this evolution is seen not only in the scope and nature of cyber security incidents, but also in the range of actors and targets," said Walter. "The 780th MI Brigade represents the Army's recognition of the cyber challenge and is charged with being part of a joint construct of cyberspace resources, creating synergy and synchronizing war-fighting effects to defend the information security environment."

Sweet also pointed out the brigade's proximity to military greatness.

"Our headquarters will lie in the shadows of two of America's most prominent general officers who spent the early parts of their military careers here at Camp Meade at the conclusion of World War I," Sweet said. "Major Dwight David Eisenhower graduated from the Camp Meade Tank School and served as commanding officer of several tank units here, and in March 1919, Major George S. Patton, Jr., commanded the 304th Tank Brigade here at Camp Meade." Eisenhower's quarters and Patton's brigade headquarters are just a few hundred yards from the 780thís eventual new home.

"Not too much pressure," Sweet added.

Prior to breaking ground for the brigade's new headquarters and operations center Sweet thanked several leaders, both in the Army and the U.S. Army Corps of Engineers, for their support in the planning and building effort.

The new headquarters is expected to be completed by the end of this year.

FORT GEORGE G. MEADE, Md. – Col. Jonathan Sweet, commander, 780th MI Brigade; Brig. Gen. Robert Walter, Deputy Commanding General, INSCOM; Fort Meade Garrison Commander Col. Edward Rothstein; Paul Karmazinski, Akima Construction; and Randy Winemiller, Baltimore District, U.S. Corps of Engineers, break ground on Feb. 23, 2013, for the 780th MI Brigade's new 46,000-square-foot facility that will serve as the brigade's headquarters.


780TH MILITARY INTELLIGENCE BRIGADE

780TH MILITARY INTELLIGENCE BRIGADE

Shoulder Sleeve Insignia

Combat Service Identification Badge

Distinctive Unit Insignia

Shoulder Sleeve Insignia. Description: On a shield shaped embroidered item, the upper corners arched inwardly, edged with a 1/8 inch (.32 cm) Yellow border, blazoned as follows: Sable, a depiction of a flowing grid Argent, charged with a disc throughout per pale Celeste (Oriental Blue) and Argent (Silver Gray) fimbriated Or, bearing a lightning bolt of the second and an arrow of the first, point upward in saltire, surmounted by a key erect, ward to sinister of the fifth, all above an arc of five mullets of the second. The overall dimensions are 3 1/4 inches (8.26 cm) in height by 2 3/4 inches (6.99 cm) in width.

Symbolism: Oriental blue and silver gray are the colors traditionally associated with Military Intelligence units. The flowing grid signifies the Brigade's link to the U.S. Cyber Command and Army Cyber Command. The modified disc suggests the unit's responsibility to provide pervasive, comprehensive, intelligence information and analysis. The combination of the shield vertically and the divided background of the disc alludes to the continuous intelligence missions and the day and night protection of cyberspace, reflecting the unit's motto "Everywhere and Always…In The Fight." The arrow symbolizes readiness; the lightning bolt denotes swiftness and the key conveys security of knowledge and truth. The five stars represent the unit's support for the Joint Forces.

Background: The shoulder sleeve insignia was approved on 6 November 2013. **(TIOH Dwg. No. A-1-1092)**

Combat Service Identification Badge: A silver color metal and enamel device 2 inches (5.08 cm) in height consisting of a design similar to the shoulder sleeve insignia.

Distinctive Unit Insignia. Description: A Silver color metal and enamel device 1 5/16 inches (3.33 cm) in height overall blazoned as follows: Sable, to dexter a waved grid and to sinister a representation of a flowing grid Argent (Silver Gray), overall a modified cryptographic disc surmounted by an algorithm encoder of the second, garnished of the first, charged with a disc per pale Celeste and Argent, bearing an arrow, point upward and a lightning bolt in saltire superimposed by a key erect, the ward upward and to sinister, all above an arch of five mullets, all of the first; issuant from base a demi-globe of the third, landmasses of the second. Attached below the device, a Black tripartite scroll inscribed "UBIQUE ET SEMPER IN PUGNA" in Silver.

Symbolism: Oriental blue and silver are the colors traditionally associated with Military Intelligence units. The shield with black background denotes protection of cyberspace. The flowing grid signifies the Brigade's link to the U.S. Cyber Command and Army Cyber Command. The modified discs suggest the unit's responsibility to provide pervasive, comprehensive information, intelligence and analysis. The demi-globe and vertically divided inner disc alludes to the continuous intelligence missions, reflecting the motto which translates to "Everywhere and Always…In The Fight." The arrow indicates readiness; the lightning bolt refers to swiftness as well as the power of cyber warfare and signal intelligence, furthermore the key conveys security of knowledge and truth. The five stars represent the unit's support for the Joint Forces.

Background: The distinctive unit insignia was approved on 6 November 2013.

Brigade Feature - our own unit identity

By Tina Miles, Public Affairs Officer, 780th Military Intelligence Brigade

IN LESS THAN 30 MINUTES, UNIT HISTORY was made for the 780th Military Intelligence Brigade as they transferred from wearing the U.S. Army Intelligence Security Command patch to wearing their own unique unit Shoulder Sleeve Insignia.

At a brief ceremony that took place April 23, on the McLaughlin Parade Field, Fort Meade, Md., the Soldiers of Headquarters and Headquarters Company, 780th MI Brigade, were charged to replace their patches. With one resounding rip of the Velcro, patches were transferred and a significant milestone in the history of the 780th MI Brigade was marked.

"Many units draw upon decades of history and a legacy of service in combat. As a new unit, operating in a new domain of warfare – we are responsible for building our legacy and creating our own unit identity, appropriate for our unique force and evolving mission," remarked Col. Jennifer Buckner, then commander of the 780th MI Brigade, when asked what the new SSI meant for her command.

Since World War I Soldiers have worn the Shoulder Sleeve Insignia to represent the identity of their unit.

"That tradition continues with the 780th MI Brigade as we begin our own history in the cyberspace domain," said Command Sgt. Maj. William Rinehart, command sergeant major, 780th MI Brigade.

The 780th MI Brigade patch itself is an embroidered shield-shaped item, with the upper corners arched inwardly. It bears a depiction of a flowing grid, charged with a disc throughout, bearing a lightning bolt of the second and an arrow of the first. Both point upward in form of a diagonal cross, like the shape of the letter X, surmounted by a key erect, ward to sinister of the fifth, all above an arc of five mullets of the second.

In symbolism, Oriental blue and silver gray are the colors traditionally associated with Military Intelligence units. The flowing grid signifies the 780th's link to the U.S. Cyber Command and Army Cyber Command. The modified disc suggests the unit's responsibility to provide pervasive, comprehensive, intelligence information and analysis.

The combination of the shield vertically and the divided background of the disc alludes to the continuous intelligence missions and the day and night protection of cyberspace, reflecting the unit's motto "Everywhere and Always…In the Fight." The arrow symbolizes readiness; the lightning bolt denotes swiftness and the key conveys security of knowledge and truth. The five stars represent the 780th MI Brigade's support to the Joint Forces.

The Army SSI was first worn in battle in 1918, and the 81st Infantry Division "Wildcat" is believed to have been the first U.S. Army unit authorized an SSI. During World War I, the 81st Division sailed for France after training at Fort Jackson, S.C. On their left shoulder the men of the division wore an olive-drab felt patch with the silhouette of a wildcat, representing Wildcat Creek, a stream that flows through Fort Jackson.

Gen. John J. Pershing approved the concept of the 81st Division's Patch, and authorized its use as a Distinctive Shoulder Sleeve Insignia. Other units followed suit, using the patches and insignias to identify their organizations and build unit pride. The Army insignia patch was elevated to an art form during World War II with symbolism and heraldry becoming the primary elements of the SSI.

The 780th MI Brigade shoulder sleeve insignia was approved by the Institute of Heraldry on Nov. 6, 2013. The 780th MI Brigade, and its subordinate units, held concurrent SSI Change Ceremonies on Apr. 23, at various locations, to officially replace their INSCOM patches with the brigade's new unit SSIs. ■

FORT GEORGE G. MEADE, Md. – Sgt. Tony Bowden, Headquarters and Headquarters Company, 780th Military Intelligence Brigade, ensure his new unit shoulder sleeve insignia, or SSI, is on straight and Staff Sgt. Michael McDonald puts away his newly replaced U.S. Army Intelligence and Security Command patch. The 780th MI Brigade, and its subordinate units, held concurrent SSI change ceremonies at various locations on Apr. 23, 2014, to officially replace their INSCOM patches with the 780th MI Brigade's new unit SSI. HHC, 780th MI Brigade, conducted their ceremony on the McLaughlin Parade Field, Fort George G. Meade, Maryland.

Happy Anniversary 780th MI BDE (Cyber)

Quotes from previous commanders and command sergeant majors

"HAPPY ANNIVERSARY 780TH MILITARY INTELLIGENCE BRIGADE (CYBER)! I feel honored to have served in this organization for six of the last seven years. As I reflect back to when I started my service to the brigade as the Command Sergeant Major of the 782d Military Intelligence Battalion (Cyber), it is amazing to see how far the brigade has progressed. When I started, not a single team had reached full operational capability and now all teams have reached that milestone. There have been changes in mission sets for some of the teams, organization into joint task forces for many of the teams, and multiple changes in training requirements in the years since. The brigade went above and beyond its responsibility of manning and equipping its cyber teams by building two joint mission operations centers, creating a team to support the tactical Army, and pooling its developers to better support requirements. These actions paved the way for the future of cyber operations across the Department of Defense. Now there are multiple joint mission operations centers, the Army stood up a battalion to provide cyberspace support to the tactical forces, and the brigade is working to build a developer detachment. The brigade continues to optimize how personnel are selected to attend advanced cyber training to ensure increased success of its personnel attending some of the most difficult training required for work role certification. It is building a pool of personnel that are certified to teach many of the required work role certification courses. Additionally, it is building four more teams over the next two years. It is exciting to be part of a fast-paced organization that continues to build and optimize for the future. I am very happy to be a member of the team and look forward to the challenges of the future to come." – CSM (Ret) James Krog

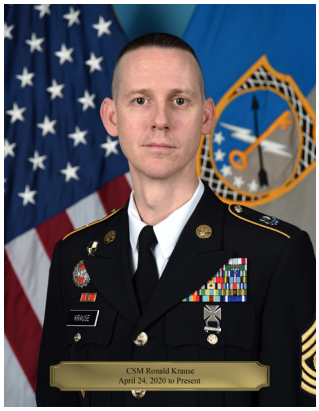
780th MI BDE Command Sergeant Majors:

CSM (Ret) Lawrence Hoke

CSM William M. Rinehart

CSM (Ret) Sheldon W. Chandler

CSM (Ret) James M. Krog



CSM Ronald V. Krause

780th MI BDE Commanders:

COL (Ret) Jonathan E. Sweet

BG (Ret) Jennifer G. Buckner

MG William J. Hartman

COL (Ret) John D. Branch

COL Brian D. Vile

COL Matthew J. Lennox

"The growth of the 780th MI Brigade I had the opportunity to 'stand-up and operationalize' back in 2011, and the mission it performs today, easily exceeds every expectation we envisioned. That's a testament to the Soldiers and Department of the Army Civilians who come to work every day with one mission in mind – get better and secure our networks. Every time I log into Facebook and see a posting of another unit being stood-up, partnerships formed with National Guard units, or a new mission being taken on, I think back to the day then-Major General Legere provided me the opportunity to take the Brigade over the finish line. Years of condition setting by many of INSCOM's finest Cyber planners and intelligence professionals was finally happening, and there we were … then-LTC Remoy and CSM Hoke, sitting at table in the old 902nd MI Brigade Headquarters, looking over a budget in the millions to train and hire analysts, build a new Brigade Headquarters, hire a Brigade Staff, stand-up a Headquarters Company, activate a Battalion at Ft. Meade and Ft. Gordon, and so much more. As they say, it takes a village, and we had the best supporting our effort. Activation Day of the 780th MI Brigade was one of the finest days in my 30-year Military Career. We built a legacy, and you continue to make it better every day! Toujours en Avant! – COL (Ret) Jon Sweet

"My time as the 780th Commander from 2016-2018, confirmed that when given hard problems and an intellectually curious and capable workforce, the common problems take a backseat (way back) to the success of the mission. Key mission challenges we faced allowed the 780th to form "family teams" that continue to support each other to this day and adapt to new tasks. I'm extremely proud to be an alum of the 780th!" – COL (Ret) Dave Branch

"Congratulations on the Brigade's tenth anniversary. The Soldiers, NCOs, Warrant Officers, Officers, and Civilians have made tremendous contributions to the defense of our nation. Since its creation, the tireless dedication and hard work of the men and women of the 780th has forged the path for other DoD cyber organizations to follow. Each member of the team has been crucial to building capability and capacity for our Army and DoD; I look forward to continuing to see the Brigade, Everywhere and Always...In the Fight!" – CSM (Ret) Sheldon Chandler

Cyber Training Battalion Activates

FORT GORDON, Ga. – The Cyber Training Battalion officially activated during a ceremony on Barton Field at Fort Gordon on October 6, 2016 with then Lt. Col. (LTC) Benjamin Sangster and Command Sgt. Maj. (CSM) Ronald Krause as the first Battalion command team. In December 2016, the Battalion was realigned under the 15th Signal Brigade. With a growth in training requirements came a growth in cadre, students, and courses leading to the activation of Bravo Company at Fort Gordon in December 2016 for all enlisted Cyber Soldiers, and Charlie Company at Fort Sill in January 2017 for Electronic Warfare Soldiers. July 2018 saw the first ever CTB Change of Command ceremony when LTC Rachael O'Connell assumed command from LTC Sangster. Detachment Corry Station stood up in July 2019, for phase one training of enlisted Cyber Soldiers. Finally, the first ever Electronic Warfare AIT course began at Fort Gordon in August 2019. On 8 July 2020, during the second CTB Change of Command Ceremony, LTC Justin Horgan assumed command from LTC Rachael O'Connell. As all EW training transitioned from Fort Sill to Fort Gordon in 2020-2021, Charlie Company deactivated at the end of 2020.

Ceremony activates one-of-a-kind battalion to support cyberspace operations

By U.S. Army Cyber Command

A NEW UNIT JOINED THE ARMY'S ARSENAL for supporting and defending its critical networks and assuring dominance in the information dimension with the activation of the 60th Offensive Cyberspace Operations Signal Battalion (OCOSB) in a ceremony at Fort Gordon, Ga., Oct. 20, 2021.

During the ceremony battalion commander Lt. Col. Kevin J. Weber and Command Sgt. Maj. Tyrone Cooper uncased the 60th's colors.

The activation marks the beginning of a new mission for the battalion, explained 1st Lt. Garrett Steinbrugge, executive officer for Company C, 60th OCOSB.

"This one-of-a-kind unit has a specialized mission to install, operate, maintain, and defend critical infrastructure and supporting networks to enable information advantage for Army and joint cyber forces," he said. "The 60th Offensive Cyber Operations Signal Battalion's unique capabilities and services will set the standard within the Army to provide robust and reliable networks supporting cyberspace effects."

But while an activation ceremony and terms such as "one-of-a-kind" imply the start of something brand new, Weber said the battalion is actually inheriting the lineage and building on the legacy of a unit with roots reaching back to before World War II.

The 60th Signal Battalion was constituted in 1933 and originally activated in 1941 at Fort Lewis, Wash. During World War II the battalion served in the Philippines, where it earned a Philippine Presidential Unit Citation before being inactivated there in 1946. Eight of its members are buried in the Philippines American Cemetery, Weber said. In 1972 it was activated again for brief service in Vietnam before being inactivated once more in California.

Col. Brian Vile, U.S. Army Cyber Command (ARCYBER) director of operations (G3), said the activation of the 60th represents the Signal Corps' assumption of one of ARCYBER's most critical missions: supporting U.S. Cyber Command's execution of full-spectrum operations.

"The Soldiers of the 60th will need to stand above their peers with their technical skills, professionalism, and ability to adapt to ever-changing situations," Vile said. "They need to be the best of the best, and the command (ARCYBER) will invest heavily in them and their mission to ensure their success."

In his remarks at the ceremony, Weber said those Soldiers are a diverse group from around the world, but all volunteered to serve and are dedicated and ready to defend the freedom of others.

"Army Cyber, we stand with you, and you stand with us, shoulder to shoulder. As of today, 60th Soldiers have boots on the ground, are engaged ... and when you see a 60th Soldier, rest assured we are protecting and defending the network," he said. ■

Lt. Col. Kevin Weber, commander of the 60th Offensive Cyberspace Operations Signal Battalion (right), and Command Sgt. Maj. Tyrone Cooper uncase the battalion's colors during an activation ceremony for the unit at Fort Gordon, Ga., Oct. 20, 2021. (Photo by Master Sgt. Teddy Wade).

Future Cyber Campus

Fort Gordon, Ga. – Aerial views show the future Cyber Campus, currently under construction. With an estimated completion date of 2029, this multi-million-dollar modernization effort is one of the DOD's largest monetary investments. Once complete, this campus will serve as the epicenter for the education and training of Army signal, cyberspace, and electromagnetic operations.

The 780th MI Brigade: Ten Years

The 780th Military Intelligence Brigade (Cyber) was activated on October 1, 2011, and officially unfurled its colors for the first time during a ceremony at Fort Meade, Maryland on December 1, 2011. The 780th MI Brigade is the only offensive cyberspace operations brigade in the U.S. Army. "Ubique Et Semper In Pugna" is latin for "Everywhere and always fighting" – We don't talk about what we do nor who we are in a cyber 'knife fight' with; however we are "Everywhere and Always... In the Fight!"

Subsequently, the 744th MI Battalion (Army Network Warfare Battalion) was re-designated as the 781st MI Battalion (Cyber) and re-organized under the 780th MI Brigade (Cyber) at Fort Meade, Maryland.

The 780th Military Intelligence Brigade (Cyber) began building a second battalion headquartered at Fort Gordon, Georgia in 2011 culminating with the stand-up and designation of the 782nd MI Battalion on June 7, 2013. Detachments Texas and Hawaii were organized as part of the 782nd MI Battalion in 2013 and 2014 respectively giving the brigade a footprint in four states in support of multiple operational headquarters.

On June 6, 2018, the Department of the Army directed U.S. Army Cyber Command to activate the 915th Cyber Warfare Battalion (915 CWB). Subsequently, ARCYBER directed the 780 MI Brigade assume Command Authority and administrative control of the 915th CWB. The 915 CWB is the first scalable organic expeditionary capability to meet the Army's current and projected tactical cyberspace requirements, including the integration of cyber and electronic warfare.

Since August 15, 2017, U.S. Army National Guard Soldiers have been mobilized and assigned to Task Force Echo, an organization conducting cyberspace operations in support of U.S. Cyber Command and the Cyber National Mission Force. The Task Force is aligned under the 780th MI Brigade, which falls under the operational control of U.S. Army Cyber Command.

"STRENGTH AND HONOR"

PRAETORIANS

780TH MILITARY INTELLIGENCE BRIGADE

NEXT QUARTER'S BYTE IS focused on AvengerCon VI. The Brigade's own hacker conference, hosted annually by a dedicated group of volunteers. They will choose this year's best presentations. As in other issues of the BYTE magazine, the command encourages your contribution to drive the Cyber and Information Advantage conversation. If you have an article to share, write a synopsis and send it to steven.p.stover.civ@army.mil NLT February 1, 2022. Final articles are due February 28.