

Volume 5, Issue 3

the BYTE

780th Military Intelligence Brigade

- * Muscatatuck UTC
- * Best Warrior Competition
- * 169 CPT: Team of Teams
- * Army Cyber Skills Challenge IV
- * Dutch Partnership
- * CyberPatriot Competition



Unity of Effort



The BYTE is a publication of the 780th Military Intelligence (MI) Brigade, Fort George G. Meade, Md.

The BYTE is an official command information publication authorized under the provisions of AR 360-1. The magazine serves the service members and civilians of the 780th MI Brigade and their Families.

Opinions expressed herein do not necessarily represent those of 780th MI Brigade or that of the Department of the Army.

All photographs published in the BYTE were taken by 780th MI Brigade Soldiers, Department of the Army Civilians (DACs), or their Family members, unless otherwise stated. The front cover and graphic posters contained within the BYTE were created by the previous Brigade public affairs officer (PAO), Tina Miles, or Steven Stover, unless otherwise stated.

Send articles, photographs or story ideas to the 780th MI Brigade PAO at steven.p.stover.civ@mail.mil, or mail to 310 Chamberlin Avenue, Fort George G. Meade, MD 20755.

For additional information, call (301) 833-6104.

Col. John “Dave” Branch
Commander

Command Sgt. Maj.
Sheldon W. Chandler Jr.
Command Sergeant Major

Steven Stover
Public Affairs Officer
and Editor



COLUMNS:

In every issue...

780 MI BDE CDR: Principles of War – Relevant to the Cyberspace Domain	1
782nd MI BN CDR: Legion 6	2
781st MI BN CDR: Team of Teams or Team of Rivals?	7
Retention	21
780 MI BDE: Hail & Farewell	22
HHC CDR 780 MI BDE: Connective Trust	27
BDE Legal: Unity of Effort vs. Unity of Thought	28
BDE SARC: Together We Can Combat Sexual Harassment and Assault	29
BDE EOA: Army Diversity: Strength in Diversity	30
BDE Chaplain: Resilience: Overcoming Challenges	33



On the Cover: Staff Sgt. Charles (Chuck) Fair, a cyber operations specialist with the 169 Cyber Protection Team (CPT), an Army National Guard (ARNG) unit, instructs Airmen from an active duty Air Force CPT as a “bridging solution” until Task Force Echo, the National Guard Cyber Battalion, assumes 169 CPT’s current mission in 2017. Additionally, there were active duty Soldiers participating in the training event.

FEATURES:

Contents

Army Cyber Unit Envisions Training and Partnership Opportunities at Indiana Urban Training Center	3
Soldiers Compete to Represent Cyber Brigade at North Regional Best Warrior Competition	5
169 CPT: Team of Teams	9
Army Cyber Warriors Compete in Annual Cyber Skills Challenge	15
Partnership between Dutch and Army Cyber Brigade Benefits Both Nations.....	19
Resilience: How applying Army resiliency in your life can help you overcome any life challenge	31
Soldiers Lead and Mentor Local High School to CyberPatriot National Finals	35

ARTICLES:

Contents

The Keys to Success: Ownership in Success, not Credit.....	8
Cyber Solutions Development: Your Mission is Our Mission	11
Shared Success Through Shared Trust	12
Training and Evaluation: Key Elements of the Build	14
782nd MI BN: Leader's week 2017	23
Fort Gordon: Unity of Effort	24
Proof of Concept – Holistic Cyber Operations Forward	25
31 Soldiers Become NCOs, Members of a Time Honored Corps	34

From the Editor

The theme for this issue is “Unity of Effort” with an emphasis on coordination and communication to achieve shared goals for success. In order to achieve unity of effort, it is necessary for each agency to synchronize their short- and long-term goals of the mission.

The theme for this issue has been directed by the Brigade commander, Col. Dave Branch. Our teams are “Everywhere and Always...In the Fight” serving under four commands and a National Command Authority; we support each of the Services; and we actively fight alongside our Joint partners and allies, to achieve U.S. supremacy in an increasingly contested cyberspace domain and electromagnetic spectrum.

On a personal note:

It is a privilege to serve as the Public Affairs Officer for the service members and civilians of 780th MI Brigade and their Families.

After 25 years of active duty service in our Army, I am truly a “Soldier for Life,” and welcome the opportunity to serve again, albeit in a different fashion, as a Department of the Army Civilian.

I am humbled by the welcome I have received, and know that I have very big shoes to fill with the retirement of Ms. Tina Miles.

v/r,

Steve Stover
Public Affairs Officer
780th MI Brigade
Editor, **the BYTE**



the BYTE: INSCOM’s nominee for the 2015 Maj. Gen. Keith L. Ware Public Affairs Competition.

The annual Department of Army’s competition recognizes Soldiers and DA Civilians for excellence in achieving the objectives of the Public Affairs Program.

Principles of War – Relevant to the Cyberspace Domain

By: Col. Dave Branch, commander, 780th Military Intelligence Brigade (Cyber)



Mass, Objective, Surprise, Security, Maneuver, Offensive, Unity of Command, Simplicity, and Economy of Force – these are the Principles of War presented by military theorist Karl von Clausewitz and then debated and studied by military leaders since. Reviewing

these principles recently, I found myself considering the Cyberspace domain and our conducted cyberspace operations over the past year in relation to these principles. For **the BYTE** audience, I wish to introduce our principles to some and remind others with the request that you too think on how these apply to our recent cyberspace accomplishments and expectations moving forward. It may to help recall the principles, using the popular phrase “MOSS MOUSE,” representing the first letter of each principle:

Mass: Concentrate combat power at the decisive place and time.

Objective: Direct every military operation toward a clearly defined, decisive, and attainable objective.

Surprise: Strike the enemy at a time, at a place, or in a manner for which he is unprepared.

Security: Never permit the enemy to acquire an unexpected advantage.

Maneuver: Place the enemy in a position of disadvantage through the flexible application of combat power.

Offensive: Seize, retain, and exploit the initiative.

Unity of Command: For every objective, ensure unity of effort under one responsible commander.

Simplicity: Prepare clear, uncomplicated plans and clear, concise orders to ensure thorough understanding.

Economy of Force: Allocate minimum essential combat power to secondary efforts.

Even in the complexity of the cyberspace domain, these

nine principles allow our force a common start point for protecting, defending, and executing offensive cyberspace operations. When I consider the Joint nature of our task forces, our tactical, operational and strategic focus points, and the broader partnerships with our interagency and Allied partners, I would offer that the Cyberspace domain may be the domain most in need of constantly applying these principles. However, in our early stages of understanding our domain and developing our force, there is a sub-principle imbedded in the principle of Unity of Command that I see exercised daily, allowing great success in planning, developing, and operating; that sub-principle is UNITY OF EFFORT (underlined above). In the newness of our force, we are teachers and students, partners and leaders, uniformed and civilian, who execute our mission with varying formations, locations, and guidance. Although uncomfortable at times, this allows the constant evolution of our abilities and accomplishments that sometimes rise and prosper from the most unexpected among us. Throughout this edition, I hope readers see the vastness of the Unity of Effort that pushes us all to better achieve our goals and provide the highest caliber service to our Nation and beyond.

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



BUTLERVILLE, Indiana -- Daniel Yeager, a cyber support technician for the Muscatatuck Urban Training Center (MUTC), Col. John (David) Branch, commander of the 780th Military Intelligence (MI) Brigade (Cyber), Command Sgt. Major Bart Larango, 782nd MI Battalion, Lt. Col. David Chang, commander, 782nd MI Battalion, and Michael King, the 782nd MI Battalion Training and Exercise director, discuss the capabilities and potential of the CyROC (Cyber Operations Center), in support of future tactical and cyber operations, on March 15. (U.S. Army Photo)

Legion 6 Farewell

By: Lt. Col. David Chang, commander, 782nd MI BN



The 782nd Military Intelligence (MI) Battalion continues to man, train, and equip the Army's Combat Mission Teams and Combat Support Teams (CMT/CST) in support of the Geographic Combatant Commands (GCC).

In the last quarter, the battalion had its final two teams complete their Full Operational Capability (FOC) exercise and were declared FOC. This completes all of the Battalion's teams and allows the Battalion to shift focus to operations and maintaining readiness. The battalion's Soldiers and civilians also had numerous operational successes over the last quarter to include the first to get to operational effects by a CMT/CST, the first to develop mission packages, and first to deliver effects synchronized with warfighter actions. There were numerous line of operations that enabled these successes.

Readiness of the Force. During the past two years, the Battalion stood up the Cyberspace Operations Range and ensured that all fourteen teams achieved FOC. The 782nd MI Battalion is committed to ensuring that all Soldiers and civilians are trained in their basic skills and maintaining team readiness by conducting realistic collective training. The battalion has developed a robust plan to recertify each team and build scenarios relevant to their real world mission set. The resources available through our Cyberspace Operations Range and our team of highly qualified assessors allow our CMT/CSTs to train as a full team and receive valuable feedback to improve team Standard Operating Procedures and unit cohesion. The ultimate goal is to ensure that the battalion's cyber teams and enablers are able to sustain a ready force able to execute directed missions in support of GCC.

Maximize the Ability to Conduct Cyberspace Operations on Service Infrastructure. Through the hard work of the Cyber Legion Soldiers and civilians, we saw the establishment of the Joint Mission Operations Center (JMOC) – Georgia. The battalion's JMOC is

working to expand infrastructure and provide training on service capabilities while certifying tool champions for internal Battalion Training. We continue to focus on real world operations utilizing service infrastructures by expanding and fully manning the JMOC.

Enhance CSCB to Support Future Tactical Operations.

In May 2016, we made the decision to establish a Cyber Electromagnetic Activities (CEMA) Support to Corps and Below (CSCB) force within the 782nd. The 782nd continues to provide support to the 780th MI Brigade's CSCB pilot under the Chief of Staff of the Army's initiative. The CSCB detachment has been conducting home station training with 2nd Armored Brigade Combat Team, 1st Infantry Division (2-1 ABCT) in preparation for National Training Center (NTC) rotation 17-06. Integration with the rotational unit exposes 2-1 ABCT to what CSCB can provide and maximizes CSCB's effectiveness during the rotation while increasing demand for Cyberspace Operational support across the force. CSCB has also been working with NTC and Ft. Irwin to set up a dedicated network for Cyberspace Operations training in conjunction with NTC rotations. In March 2017, we officially stood up the Expeditionary Cyber Support Detachment and assumed the lead effort for the 780 MI Brigade.

Govern the Development of Cyber Tools and Capabilities.

In January 2016, we stood up the Effects Support Cell (ESC). The Battalion's ESC continues to grow in size and capabilities. Work has begun to expand the ESC's infrastructure in order to enable operations by an adaptive, resilient network, systems, weapons platforms, and tools that rapidly integrate innovative and advanced technologies. The ESC also provides support to competitions such as the "Drone Wars" hacking challenge that took place during the recent Battalion Leaders' Week.

I want to close by saying it has been a privilege and an honor serving the Soldiers and civilians of the 782nd MI Battalion as your commander. You, the Cyber Legion, are making history every day. Everywhere I go, senior leaders at every echelon are amazed at the requirements and standards you achieve everyday through your hard work and discipline. My family and I have enjoyed being a part of this incredible organization. I am honored to have been your commander, and enjoyed working with you every day.

CYBER LEGION!

Army Cyber Unit Envisions Training and Partnerships

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



Daniel Yeager, a cyber support technician for the Muscatatuck Urban Training Center (MUTC), near Butlerville, Ind., briefs Col. John (David) Branch, commander of the 780th Military Intelligence Brigade (Cyber), on the capabilities of the CyROC, a Cyber Operations Center, in support of tactical and cyber operations, on March 15. (U.S. Army Photo)

BUTLERVILLE, Indiana – The Muscatatuck Urban Training Center (MUTC), facilitated and managed by the Indiana Army National Guard (ARNG), is a thousand-acre advanced urban training facility with over 200 buildings that the Chief of Staff of the Army saved from being bulldozed in 2005 – during the height the Iraq war – because the Army needed a place to conduct urban training.

Today, Muscatatuck is not only used by the military, but by first responders – police, firefighters, emergency medical technicians – as well as federal agencies, such as the Department of Energy. Other countries have sent their people to train here too.

According to Lt. Col John Pitt, commander of the Muscatatuck Urban Training Center, and battalion commander of the 113th Engineer Battalion, Indiana ARNG. “Everything here is in play.”

“It’s a facility focused on a training environment for live virtual constructive testing, training, and evaluation. It a best value solution,” said Pitt. “It’s for anyone chartered with ‘protecting the homeland, winning the peace.’”

To emphasize his point, Pitt said in addition to host-

ing the State police, K-9 units, and search and rescue teams, the Navy ran an exercise where a V-22 Osprey, a joint service, multi-mission aircraft with vertical take-off and landing (VTOL) capability, lifted off from a carrier in the Atlantic Ocean, flew over several States to MUTC, and then conducted a U.S. Embassy strengthening operation.

The 780th Military Intelligence (MI) Brigade (Cyber) sees great potential in conducting training and testing for cyberspace operations at Muscatatuck, complementing ongoing efforts to construct permanent cyber training infrastructures at the Army’s Combat Training Centers.

“We’re looking for an enterprise capability. Maybe a potential for offensive and defensive (cyber) working together in this environment in the future.”

“We’re looking for an enterprise capability. Maybe a potential for offensive and defensive (cyber) working together in this environment in the future,” said Col. John (David) Branch, commander of the 780th MI



BUTLERVILLE, Indiana -- (left to right) Daniel Yeager, a cyber support technician for the Muscatatuck Urban Training Center (MUTC), Lt. Col. David Chang, commander, 782nd Military Intelligence (MI) Battalion, Michael King, the battalion’s Training and Exercise director, and Lt. Col. John Pitt, MUTC commander, discuss potential cyberspace and tactical training opportunities with Col. John (David) Branch, commander, 780 MI Brigade (Cyber), inside of a prison and courtroom facility, on March 15. (U.S. Army Photo)

Opportunities at Indiana Urban Training Center



Lt. Col. John Pitt (bottom left), commander, Muscatatuck Urban Training Center, takes Col. John (David) Branch, commander of the 780th Military Intelligence Brigade (Cyber), and other brigade leaders, on a tour of the various Urban Training Zones, to include a multi-story hospital, fresh-water and waste-water treatment facilities, a coal-fired steam plant, an embassy, high school, and even a prison, on March 15. (U.S. Army Photo)

Brigade. “The Muscatatuck training site is maturing, it’s getting some recognition, so we need look and see if that’s a future tactical training site for us or an operational training site.”

As he escorted the brigade team Pitt commented that, “One of the things Muscatatuck offers that no other place offers is the complexity and the completeness of electronic environment with infrastructure. There will be plenty of labs out there with a computer going against another computer – and a network cable between the two, or maybe a server between the two, but never with the integrated environment and infrastructure where it’s a computer going through a network to a SCADA (Supervisory Control and Data Acquisition) device with something after that SCADA device or that HMI (Human Machine Interfaces) that takes electronic symbol and turns it into a physical action. There is no other place with the level of complexity and integration between the electromagnetic and physical environment.”

One of the Urban Training Zones the brigade toured was an urban zone called the CyberTropolis. The zone consists of a representative city and residential infrastructure outfitted with operational SCADA, cellular, and enterprise networks. Within CyberTropolis, is the CyROC, a Cyber Operations Center, the command and control (C2) center for area. The MUTC staff can also provide personnel to fill the following roles: Red

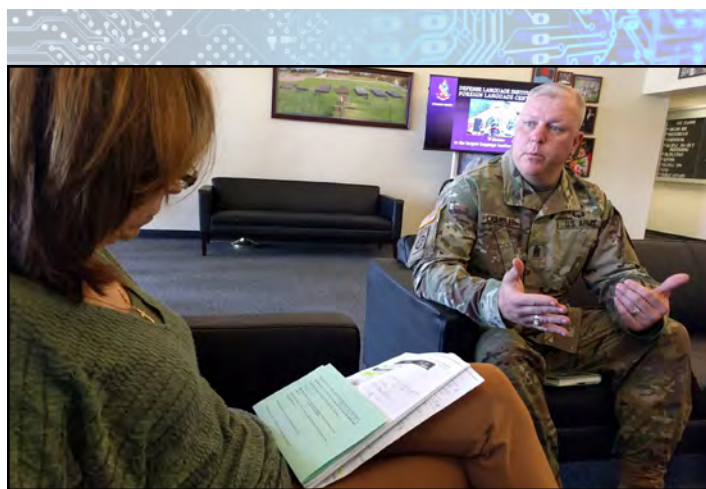
Team (enemy), Blue Team (friendly), Insider Threat Gray Team, Supervisory White Team, and Assessment, as well as the necessary work space and computing resources to conduct their roles in testing, training or developmental cyber operations.

The brigade team agrees, there is potential and capabilities not found elsewhere.

“I can remember training at another site where our Red Cell guys were sitting in a CONEX with a laptop and we had to put in our own WiFi router, it’s all here already,” said Lt. Col. David Chang, commander, 782nd Military Intelligence Battalion. “A lot of our concerns for a real-world environment are better emulated here because of the complex environment.”

Eventually, Branch wants to bring out his bosses to see an exercise where a tactical unit is supported by one of his cyber teams.

“My higher headquarters wants me to move towards tactical cyber, so I need to determine what is in the realm of possible,” said Branch. “CSCB (Cyber Electromagnetic Activities (CEMA) Support to Corps and Below) efforts, working with other elements, working with divisions, corps, this is what we’re talking about.”



MONTEREY, California -- Command Sgt. Maj. Sheldon Chandler of the 780th MI Brigade, visited the Defense Language Institute Foreign Language Center March 23-24. Chandler took the opportunity to find out more about the foreign language learning process at the institute and visited basic course classes, intermediate and advanced programs. (U.S. Army Photo)

Soldiers Compete to Represent Cyber Brigade at N

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



FORT GORDON, Georgia – The 780th Military Intelligence (MI) Brigade competitors for the brigade's 2017 Best Warrior Competition, from left to right, Spc. Alan Kim, Headquarters and Headquarters Company (HHC), 780th MI Brigade; Sgt. Jonathan Porter, Detachment Hawaii (DET HI), 782nd MI Battalion; Spc. Johnny Long, DET HI, 782nd MI Battalion (brigade's BWC Best Warrior, Soldier); Spc. Savannah Matelski, Delta Company (Co.), 781st MI Battalion (brigade's BWC Soldier, runner-up); Staff Sgt. Scott Stappenbeck, Charlie Co., 781st MI Battalion (brigade's BWC Noncommissioned Officer (NCO), runner-up); and Staff Sgt. Humberto Gutierrez, HHC, 780th MI Brigade (brigade's Best Warrior, NCO), April 21. (U.S. Army Photo)

FORT GORDON, Georgia – In preparation for the 2017 Department of the Army Noncommissioned Officer (NCO) of the Year and Soldier of the Year Best Warrior Competition (BWC), Soldiers from the 780th Military Intelligence (MI) Brigade competed in the brigade's BWC April 16 to 21.

Staff Sgt. Humberto Gutierrez, Headquarters and Headquarters Company (HHC), 780th MI Brigade, and Spc. Johnny Long, Detachment Hawaii, 782nd MI Battalion, will represent the brigade as it's best warriors and compete against representatives from the 704th MI Brigade, 902 MI Group, Army Field Support Center, Army Operations Group, 1st Information Operations Command (Land), and HHC U.S. Army Intelligence & Security Command (INSCOM) at the INSCOM 2017 North Regional BWC in mid-May.

According to Sgt. Maj. Jesse Potter, operations sergeant major for the 780th MI Brigade, the BWC is a fairly new event. Prior to 9-11, organizations held a panel

board to select the NCO and Soldier of the Year to represent their respective units.

"After 9-11, Sergeant Major of the Army, Kenneth Preston, said this selection process is not realistic. This is not realistic of the Total Soldier concept and it is not very realistic of our Army," said Potter at the brigade's BWC selection ceremony. "The Army established the Best Warrior Competition to identify the best warrior. You're not going to be the NCO of the year, or Soldier of the year, you're going to be the best warrior for the Army."

"You're not going to be the NCO of the year, or Soldier of the year, you're going to be the best warrior for the Army."

The brigade's week-long event was both physically and mentally challenging.

Many of competitors said the ruck march was the toughest physical challenge and that the panel board was the toughest mentally; however, both the best warrior NCO and Soldier said it was the competition that was the toughest.

"The most challenging event overall was the ruck march," said Long. "It wasn't because they gave us a particularly tough ruck route or the distance. It was because the competition was really steep."

Gutierrez, the brigade's NCO best warrior, spoke about the camaraderie amongst the competitors and how, even though they were competing against each other, everyone was willing to help each other as well.

"It was great working with them. I enjoyed the competition," said Gutierrez. "I really hope to see them all next year."

For each competitor, it was an honor to represent their unit and their fellow Soldiers, but for Long and Gutierrez their job isn't over.

"It means there's more fun to be had, more travel, new experiences," said Long. "Ultimately it means I have a lot more to do in the next couple of weeks, because with

North Regional Best Warrior Competition



FORT GORDON, Georgia – Staff Sgt. Humberto Gutierrez, Headquarters and Headquarters Company, 780th Military Intelligence Brigade, will represent the brigade as its best warrior in the noncommissioned officer category at the U.S. Army Intelligence & Security Command 2017 North Regional Best Warrior Competition in mid-May. (U.S. Army Photo)

some of those events, I have a lot of ground to cover if I'm going to be competitive."

Gutierrez summed up his goal for the INSCOM 2017 North Regional BWC Competition.



"I'm just seeing another mountain...another mountain to climb over. And looking back at this one, seeing I could do it."

The competition started with an APFT, and over the next four days included the following: 20 Army Warrior Tasks; a written essay and exam; disassembling, reassembling, and performing a functions check on an M9 pistol and M4 rifle; M4 zero and qualification; land navigation; a 12-mile road march; an operational fitness challenge consisting of four iterations of 800 meters on a rowing machine, 40 Army PRT (physical readiness training) rowers, and 70 push-ups, followed by pushing and pulling a 200 pound sled, within a one-hour time limit. The competition concluded with a panel board.

Though there was some disappointment for those not making it to the next level, Command Sgt. Maj. Sheldon Chandler, 780 MI Brigade, told all the competitors at this level, they are all winners.



FORT GORDON, Georgia – Spc. Johnny Long, Detachment Hawaii, 782nd Military Intelligence (MI) Battalion, will represent the 780th MI Brigade as its best warrior in the Soldier category at the U.S. Army Intelligence & Security Command 2017 North Regional Best Warrior Competition in mid-May. (U.S. Army Photo)

Team of Teams or Team of Rivals?

By: Lt. Col. Justin Considine, commander, 781st Military Intelligence Battalion (Cyber)



“A house divided cannot stand.”

– Abraham Lincoln

As the Brigade marches toward the Army’s objective of becoming the first Service to achieve Full Operational Capability (FOC)

for all assigned and attached Cyber Mission Force (CMF) teams, we continue to steer the transition from a ‘build’ phase to an ‘execution’ phase in which we sustain our manning and training levels while increasingly focusing our efforts on Mission Readiness. However, when it comes to building unit identity and organizational culture, we are very much still in a ‘build’ phase. Even as we demonstrate our ability to deliver effects against our adversaries in cyberspace, we wrestle every day with the competing priorities and requirements of the operational and administrative commanders. So how do we cultivate unity of effort without unity of command?

Eight months ago when I assumed command of the Vanguard Battalion, we applied the simple yet powerful value of ‘starting with why’ – defining the purpose of the organization to foster an environment in which great things can happen. First, we started with our name – the Vanguard, defined as a forward element, leading from the front, blazing the trail, informing those who would follow behind. We solicited input on the Vision of the Vanguard – the essence of WHO we are: an elite cyberspace maneuver force, always out front and in the fight, using technology as a weapon system to defend the nation. We highlighted our values, and together we developed an ethos of HOW we will live by these values – to be a professionally led, technically superior, operationally engaged, organizationally adaptive, intellectually innovative, and holistically resilient TEAM of TEAMS. But how do we foster teamwork without the strong communication, regular engagements, and constant partnership that sows shared understanding and shared purpose?

Our minds, like our bodies, can be conditioned into a way of performing and behaving. The OPCON (Operational Control) and ADCON (Administrative Control) split that may work effectively in the Military Intelligence Corps or other operations support branches is less tenable in an operations branch such as Cyber. Strict adherence to a division of roles and responsibilities breeds a toxic ‘us and them’ dynamic that undermines the cohesion critical to the effective employment of combat forces. As Maj. Danielle Gonzalez, 01 National Mission Team Lead, writes, “Retooling the way people in an organization think of themselves and each other is a significant component of building (or rebuilding) the organization’s foundation. Building unity of effort in an organization can be likened to building a house on a strong slab of concrete, on a solid piece of earth. Building unity of effort within an organization must occur after the organization sees themselves as one team, composed of people who see differences among people as strengths rather than weaknesses.” So how do we build the foundation of teamwork which is vital to unity of effort when the operational and administrative commanders have unsynchronized and often competing perspectives?

“As a cyberspace maneuver force, it is imperative we see ourselves as a cohesive combat unit.”

As a cyberspace maneuver force, it is imperative we see ourselves as a cohesive combat unit. In a hybrid operating environment in which real world operations are conducted 24/7/365, it is arguably archaic to think that Service components can ‘turn over’ their forces to an operational commander when we are not deploying for set periods of time and resetting in accordance with an established force generation model. As Lt. Col. Chris Longo, deputy brigade commander, 780th Military Intelligence (MI) Brigade (Cyber), contends, unifying the command structure at the brigade and below levels normalizes our structure with other Army maneuver forces and adheres to the “Army’s regulations, policy, and doctrine that have been developed over the course of

over 200 years of experience of those who have come before us.” Our goal, therefore, must be a framework in which commanders are empowered to assess risk to operations and make decisions to accomplish the mission based on the assessed risks. This shared view, as Army Capt. Iain Cruickshank, commander of Delta Company (Co.), 781st MI Battalion, call sign Delta Legion 6, asserts, is “absolutely foundational to creating unity of effort.” But how do we unify our efforts when we are embattled with the tyranny of dispersed locations and split-based mission command?

Until we have the shared space of a unified setting that affords teams the opportunity to conduct operations as complete teams (currently only experienced in short exercises), and until we have the shared view of unified command as the optimal mission command solution, we will nonetheless continue to advocate for the shared consciousness needed to overcome the “prisoner’s dilemma” that incentivizes competition over cooperation. As we build towards our vision of being an operational maneuver force, we will unfailingly accomplish our assigned missions, albeit as ‘catalysts’, concludes Capt. Eric Zastoupil, commander of Charlie Co., 781st MI Battalion, call sign Conqueror 6, and “fulfill our responsibilities to the operational command by providing a professional maneuver force prepared to fight and win the nation’s wars in cyberspace.”

“Vanguard! When Others Cannot!!”

The Keys to Success: Ownership in Success, not Credit

By: Capt. Skylar Onken, Sub-Element Lead, 61st National Mission Team, Alpha Company, 781st MI Battalion

I once heard a story about a group of men attempting to move a grand piano by hand. None of the men were professional movers, and the task was truly daunting.

It was evident to all of the men that the task would not only require feats of strength, but also careful planning and organization. Attempt after attempt failed to move the piano in a way that produced any real results. No matter how they organized or ordered the group, they could not balance the piano while providing the strength necessary to move it. Just as they would lift

the wider and heavier end, the opposing side would tip and hit the floor. Conversely, lifting the narrower end first only made it harder to lift the wider portion.

Those of you who have moved a piano can immediately empathize with these men and the difficulty of the task. I can imagine the people in this group - the brawny ones with their wide set weight-lifting stances, the tall ones trying to bend over awkwardly, and the smaller individuals, lifting only half-heartedly.

In the end, one of the men suggested they stand shoulder-to-shoulder, and each man simply lift their portion as best as they could. Although slightly uncomfortable, they were able to fit more of the group into the task at



hand. In spite of their reservations, all of the men immediately saw the results of their combined efforts. They were able to accomplish more, and with less individual effort, than they had previously thought.

I am sure that many of the men had their misgivings. I imagine that the strongest of the group was likely convinced that if he were given more space he could have lifted more than any other man. Similar sentiments were likely shared throughout; however, in the end, it was proven that only when working as a cohesive unit were they able to accomplish their mission.

I believe we can learn a lot from this allegory. We are an organization rich with talent. We have technicians, leaders, organizers and others with various skills sets. Often we become invested in a specific task or project and begin to feel ownership over it. Such ownership is vital for the success of a mission. However, there is also a danger in becoming defensive of that task. In these situations we may compromise the mission by excluding ideas and people who can offer great value.

(Continued on page 13)

Unity of Effort in Cyber Operations: Team of Teams,

By: Capt. Christie P. Cunningham, commander, Headquarters and Headquarters Company, 781st MI Battalion



169 Cyber Protection Team, an Army National Guard unit, is a 'team of teams.' The unit is a cyber operations team comprised of National Guard Soldiers from 19 states and territories, and is augmented with personnel from the Headquarters and Headquarters Company, 781st Military Intelligence Battalion (Cyber). (U.S. Army Photo)

As the world becomes increasingly complex and the Department of Defense (DoD) works to address threats across the globe, Army leaders must emphasize unity of effort to enable multiple organizations to complement one another while balancing myriad priorities in order to maximize mission success.

However, traditional paradigms that guide unity of effort – temporal/geographical milestones that guide command primacy, working groups, and planning committees – cannot alone empower effective unity of effort for cyber operations. The cyberspace domain spans all physical domains, and cyber warriors can conduct operations from anywhere in the world. Multiple affected units and partners must balance mission requirements with a single pool of assets in an environment that is simultaneously “home station” and “deployed.”

Thus, a new paradigm is required – one that cultivates a team of teams, and a network of networks – building relationships and processes that benefit all the commands involved. This effort is critical for current operations and for developing adaptability that will enable cyber warriors “to be able to fight tonight, but to also fight tomorrow.”

The establishment, training, and operational capabilities of 169 Cyber Protection Team (CPT), a National Guard (NG) unit attached to the Headquarters, and Headquarters Company (HHC), 781st Military Intelligence (MI) Battalion, is a perfect example of the Total Army unity of effort for cyber operations.

169 CPT was established in October 2013, following a Concept Plan between the Headquarters, Department of the Army (HQDA) G3/5/7 and the National Guard Bureau (NGB). The NG has augmented Active Army units in the past to support cyber operations; however, this was the first large-scale organized effort to establish the Total Army concept for cyber forces. 169 CPT is comprised of 39 personnel from 19 different states. Generally, NG Soldiers work part-time, in their M-day capacity (M-day refers to the regular weekend drilling Soldiers), but Soldiers on 169 CPT were brought onto active duty orders (active duty operational support – reserve component/ADOS-RC) for the purposes of this pilot program.

Though 169 CPT is attached to HHC, 781st MI Battalion, the battalion shares administrative control of the team with NGB, and with the individual states to which team members are assigned (in their M-Day capacity). Furthermore, the 780th MI Brigade retains operational control of the team.

169 CPT is the first NG CPT charged with executing a mission that required unity of effort across multiple



Staff Sgt. Charles (Chuck) Fair, a cyber operations specialist with the 169 Cyber Protection Team (CPT), an Army National Guard unit, instructs Airmen from an active duty Air Force CPT as a “bridging solution” until Task Force Echo, the National Guard Cyber Battalion, assumes 169 CPT’s current mission in 2017. (U.S. Army Photo)

and Network of Networks

Army components. Army leaders from HQDA and NGB envisioned the team would eventually conduct training and operations that met NG goals of building an expert cyber force, to include a newly-developing NG Cyber Brigade – though a partnership with the active Army – while concurrently enabling priority missions for the active Army and U.S. Cyber Command (USCYBERCOM).

According to Army Capt Nico Smith, a Computer Network Defense (CND) manager for 169 CPT, employing a NG element in this manner has brought unique administrative challenges, but having a cache of untapped talent from civilian careers cannot be easily replicated elsewhere.

“In order to accomplish the missions to which we were aligned, members from the team pulled from their civilian-acquired skills. In the private sector, team members worked as systems engineers and penetration testers for organizations like state utilities agencies, Microsoft, Nintendo, Fire-eye, and HP (Hewlett Packard),” said Smith. “Experience, professional development, and exposure to industry standards and process management in the private sector gave team members expertise about red teams and cyber intelligence before those were well-known concepts across DoD.”

Army Maj. Mathew Taylor, another CND Manager for 169 CPT, said the 781st MI Battalion and 169 CPT successfully navigated these complex challenges through developing shared understanding across multiple partners, and aligning tasks and efforts to exploit points of synergy.

169 CPT has worked with active Army units to train; conduct defensive cyber operations, cyber command readiness inspections, vulnerability assessments, and cyber OPFOR (Opposing Force) support; as well as developing coursework for the NG Professional Education Center. The team also developed training courses to improve Soldier, Airman, Sailor, and Marine proficiency across active and Reserve forces, and developed a first-of-its-kind unique capability that provides the USCYBERCOM commander the ability to conduct full-spectrum cyber operations.

Through their efforts, the team simultaneously achieved the goals of Army leaders from the NGB, active Army, and the Joint Services – they enhanced the readiness posture of Cyber Forces, becoming the first National Guard CPT to achieve initial operational capability (IOC) in 2016.

The 781st MI Battalion and 169 CPT have proven that a unity of effort framework of aggressive learning, collaboration across partners, and deliberate efforts to find points of synergy can accomplish goals of multiple organizations at the same time.

This broader team approach continues the Total Force solution in the cyber domain – 169 CPT is training an active duty Air Force CPT on its current mission set, and will soon be integrating Task Force Echo, a battalion-sized element within the now-established NG Cyber Brigade, to be the first of multiple elements responsible for the USCYBERCOM capability originally developed by 169 CPT. The collective team’s push for unity of effort across multiple components has directly shaped the Total Force paradigm for cyber force optimization in the cyber domain.

Clearly, cultivating unity of effort within the cyber community is a difficult feat due to challenges focused on command primacy, balancing administrative and operational requirements with one pool of resources, and the ever-evolving cyber environment. The key to cultivating unity of effort within this field has been in finding points of synergy across our environment and reaching out to “connectors” who might further enable our collective success. In short, unity of effort across the cyber community relies upon building a team of teams, and developing networks of networks.



Soldiers and civilians associated with 169 Cyber Protection Team, and the Headquarters and Headquarters Company, 781st Military Intelligence Battalion (Cyber), recently competed in a team building event, a Spartan Race, to build esprit de corps and camaraderie. (U.S. Army Photo)

Cyber Solutions Development: Your Mission is Our Mission

By: Capt. Alex Eubanks, developer, Cyber Solutions Development Detachment, 781st MI Battalion (Cyber)

The 781st Military Intelligence (MI) Battalion Cyber Solutions Development Detachment, or CSD, is one of the newest subordinate elements under the 780th MI Brigade (Cyber). The CSD works with multiple organizations and cyber teams across the brigade, U.S. Cyber Command (USCYBERCOM), and the Department of Defense (DoD), to bring critical low-density development skills to bear against a wide-range of technical challenges.

Typically, working in a supporting role, not all of the supported organizations are aware of the detachment's general abilities in development, what is available to the 780 MI Brigade and Cyber National Mission Force (CNMF), and how we are assisting others accomplish their mission.

At the basic level, all cyber Soldiers and leaders have some development ability, whether it be two weeks of Python (a programming language) training through the Joint Cyber Analysis Course (JCAC), programming courses taught through the cyber school house, or additional experience gained through individual instruction and training. However, cyber teams could find themselves crunched for time or without the specific skill set required to accomplish an operation, and this is where the CSD can assist.

The CSD is one of several development organizations. For example, the 782nd Effects Support Cell (ESC), co-located with the 782nd MI Battalion headquarters, supports units at Fort Gordon.

Both development organizations have consolidated Soldiers, non-commissioned officers (NCOs), warrant officers and officers, with decades of experience in assembly and C-programming, software reverse-engineering, hardware design and reverse-engineering, framework construction, and the ability to create capability, beyond what is taught through the Army's traditional (cyber training) pipelines.

The CSD has four main lines of effort (LOE): The Army's Platform Mission Assurance mission, support to the Cyber Mission Force, support to Cyber Electromagnetic Activities (CEMA) Support to Corps and Below (CSCB), and support to contingency opera-

tions. The CSD creates a variety of custom-tailored software and hardware solutions for members of the DoD, primarily the Army, in support of their efforts. If an organization is conducting cyberspace operations within the 780th MI Brigade, and their operations fall within one of the LOEs above, they should contact the 781 CSD or 782 ESC.

The 781 CSD job is to support their customers, and not their customers' job to be supported by the CSD. One way the CSD is moving forward with a "support the fight" mentality is through an outreach program. Junior leaders from the CSD are going forward to meet with teams directly in order to understand their problems, and learn which of these problems the CSD team can help resolve. The purpose of this outreach is to knock down the barriers to effective communication.

Support from the CSD begins with a conversation. Customer organizations who do not currently have a point of contact with the CSD, should work through the (781st MI Battalion) chain of command and, once approved, the CSD will send out a representative. Each of the CSD representatives understand the detachment's workload, what they can bring to the fight, and each are empowered to integrate with the supported cyber teams, plan their support, and make decisions.

While members of the CSD are aware of the capabilities currently available to teams through USCYBERCOM resources, the purpose of the CSD is to help identify the critical capability gaps required for mission accomplishment. Simply, the CSD works with supported elements to custom-tailor solutions.

Once the CSD representatives have put together a viable plan, they meet with CSD leadership and pitch ideas on behalf of their supported elements. CSD leadership, with an understanding of requirements across the CSD, align personnel and resources, requests support from higher headquarters when appropriate, and supervises the implementation of capability. If the CSD is not the right organization to implement the capability, but

(Continued on page 13)

Shared Success Through Shared Trust

By: Capt. Alex Farmer, Echo Company, 781st Military Intelligence Battalion

Units supporting Combined Joint Task Force-Operation Inherent Resolve (CJTF-OIR) have been conducting Counter-ISIS (Islamic State in Iraq and Syria) advise, assist, and accompany operations in Iraq and Syria since 2014. Since then, those units supporting CJTF-OIR have been on a constant rotation of support and have gained a significant amount of experience in modern warfare. These forces have experience fielding and integrating cutting edge technologies that can shape the battlefield.

These deployed units also foster a bottom up driven leadership model which relies on trust, builds on failures, and ultimately achieves a high confidence of mission success when the mission is of critical national importance. If the 780th Military Intelligence (MI) Brigade wants to provide forces in cyberspace to be called upon when Americans' lives are at stake, the organization must learn from these experiences.

How do relationships with the U.S. Special Operations Command (SOCOM) and the ground forces of the Army achieve an operationalized Cyber unit?

Over the past two years, I have gained valuable experience augmenting SOCOM units in a garrison and forward deployed capacity. This article will provide several use-cases that illustrate how linking with other flexible and adaptive units in the military has increased the effective capability of the 780th MI Brigade. Ultimately these examples illustrate how the brigade, as a whole, is unified through support to deployed operations and is engaged in solving the cutting-edge problems that define the cyberspace domain for the Army.

Cyberspace operations require flexibility and agility – above that of traditional warfighting domains – when it comes to the fielding of capabilities and the execution of effects that rely on fleeting opportunities to create real operational impact.

The 780th MI Brigade's newly formed Cyberspace Solutions Development Detachment (CSD) recently fielded and delivered a capability to deployed forces in less than eight months. CSD takes advantage of a critical mass of intelligent and dedicated Soldiers

who provide development support to their deployed counterparts. A deadly capability gap was answered because a forward deployed planner had trained in cyberspace operations and could rapidly identify an opportunity to bring the brigade into the fight.

By leveraging development cells across the Army, the Department of Defense, and the Intelligence Community, the CSD had a capability ready for local testing in three months and fielded to deployed forward units in five months. Only eight months after the initial concept, an operational capability was delivered on a small scale. This was only the first iteration of these processes, and CSD development support, speed and quality, will continue to improve as the detachment gains in experience.

The 780th MI Brigade support to SOCOM and special operations in general is only a smaller subsection of the Cyber Electromagnetic Activities (CEMA) Support to Corps and Below (CSCB) concept. Through direct support to units at the battalion-level, the Brigade has proven that groundbreaking achievements can occur with the right level of support. These achievements and lessons are gained through experience in deployment and distributed to the Army at training events and exercises.

These exercises also provide an opportunity to build relationships and the trust necessary to create effective operational impacts. The experience gained in development and deployment of a sensor at the National Training Center (NTC) provided the basis for a capability currently deployed in Syria. Experience from the operational employment is informing redesign for capabilities planned for use in the upcoming NTC rotation. These operations support interrelated and interdependent missions that ultimately provide lessons across an extensive subset of the cyberspace domain.

The staff and their processes also grow more capable with each event, whether operational or exercise, and collectively this makes the brigade more prepared to answer those mission critical requirements. Each

(Continued on page 13)

Keys to Success

(Continued from page 8)

Similarly, some people in the unit demonstrate unprecedented skills and capacity in certain areas. Just as this talent can lead to incredible results, it can also result in overinflated egos. In these situations, we may not allow space for others to help in our efforts. No matter how great the talent, it will never accomplish what a cohesive team could do.

If you find yourself in this category, rest assured that there is plenty of room around the metaphorical piano. Each Soldier and civilian has unique talents and skills to contribute.

At the last Battalion Town Hall, Lt. Col. Justin Considine, the commander of the 781st Military Intelligence (MI) Battalion, discussed the concept of givers and takers. During this discussion I kept thinking about how the mission of an organization can create an environment that encourages either giving or taking. Each individual's words and attitude contributes to the environment. If we become too focused on what we can get from the Army, or not getting the praise we think we deserve, we will start to emote and spread that toxic attitude amongst our peers. In the end this compromises our ability to act, as a team, and America cannot afford for us to lose sight of the important mission we are responsible for – The 781st MI Battalion conducts cyberspace operations and signals intelligence to create operational effects in and through the cyberspace domain to gain and maintain freedom of action required to support Army and Joint requirements while denying the same to our adversaries.

I hope that each of us can come to work each day eagerly looking for a task to complete or a need to be met. Just as the men from the story, no single person can move a piano on their own. Each person contributed to the burden and balance of the task from a different perspective and position. Similarly, we each must recognize the value that we provide is only truly recognized when the success of the team is measured as a whole.

CSD: Your Mission is Our Mission

(Continued from page 11)

another development effort is, the requirement may be directed to another development effort. If additional information, official request forms, or other administrative actions are required, the CSD works with supported elements – it is a shared process.

The desired end-state of a CSD mission is new capability, custom-tailored to the needs and requirements of a supported element, on short-to-medium time scales, to meet operational timelines. The CSD works with the supported elements throughout the development timeline to ensure what they deliver meets their requirements.

The CSD maxim is “Your mission is our mission,” and the CSD is here to support elements across the 780 MI Brigade, USCYBERCOM, and the DoD, in order to accomplish the mission.

Shared Success, Shared Trust

(Continued from page 12)

operation that occurs in any of the above mission areas depends heavily on this relationship and collective learning that is military operations in cyberspace.

The 780th MI Brigade is at the forefront of execution in the cyberspace domain and is taking an active role in understanding what the reality of cyberspace operations looks like. It can be challenging to answer the ultimate ill-defined problem ‘do the cyber’ but through learning from failure and seeking out opportunities in conjunction with deployed forces the collective effort makes significant forward progress. Like our deployed partners, we must rely on trust in each other, build on our failures, and ultimately achieve a high confidence of mission success when the mission is of critical national importance.



Training and Evaluation: Key Elements of the Build

By: Tracy Manassa, Operations (S3) Cyber Planner, 780th MI Brigade (Cyber)

Training and evaluation are key elements of the build, employment and sustainment of mission-ready forces. The Cyber Mission Force (CMF) requires clear standards and guidelines to ensure that all teams have the skills and training needed to successfully accomplish their identified missions.

Cyberspace has added a new dimension to modern warfare. Forces necessary to fight and win in cyberspace face extraordinary mission demands in maintaining the integrity of the domain as well as projecting national power and defeating adversaries. The Department of Defense (DoD) decided there was a requirement to provide highly-trained and mission-ready forces specialized to meet these mission demands and the significant challenges outlined in the Cyber Force Concept of Operations and Employment – DoD must develop a trained and ready CMF.

As part of the 780th Military Intelligence (MI) Brigade mission to man, train, and equip the Army's first cyber teams – The brigade's Training and Exercise (TREX) section and Scenario Development Team (SDT), which is comprised of subject matter experts (SMEs) from across the 780th MI Brigade, along with SMEs from U.S. Marine Forces Cyber, and Fleet Cyber, shifted their focus to building extensive and well-designed scenarios tailored to each team's mission. The scenario is a 3000/4000 level collective training event that requires all work roles of the team to work together toward a common objective.

Members of the SDT met for two weeks and created scenarios that are synchronized with the U.S. Cyber Command training and readiness manual's Mission Essential Tasks (METs). Lt. Col. Jesse Sandefer, the 780th MI Brigade operations (S3) officer-in-charge, provided the following guidance to the SDT.

"The scenario should be a based scenario with: threads that create a robust and real world like scenario that incorporates all work roles; there should be multiple lines of efforts and all supporting and required documents such as operations orders, annexes and serialized reporting will need to be available; and a full 10 days

of injects that will give the team the flexibility to have ad hoc injects throughout the exercise. "

Going forward, the SDT developed a brigade validation exercise scenario that is robust and effectively incorporates all the work roles of a National Mission Team / National Support Team or Cyber Mission Team / Cyber Support Team, and can be used to assess all Training and Readiness METs. The scenario and target environment was developed as a single overarching scenario with four different threads that allows teams to choose a thread that is closer to resembling the team's real-world mission. By doing this, the scenario and target environment is capable of supporting a single team conducting a stand-alone validation exercise or up to four teams and a higher headquarters exercising simultaneously as part of a cyber Soldier exercise.

In January cyber team members from the Army, Air Force and Navy conducted a collective training exercises. The following excerpt is from team's After Action Report:

(Continued on page 26)



1st Lt. Stephen Rogacki (right), a cyber operations officer, Bravo Company, 781st Military Intelligence Battalion (Cyber), and Staff Sgt. Gerald Topel, a cyber operations specialist, are coordinating offensive cyber operations in order to attack an adversary spaceship and command center during Iron Castle Space, a cyber wargaming exercise. (US Army Photo)

Army Cyber Warriors Compete in Annual Cyber

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



Chief Warrant Officer 4 Kirk Bond, 780th Military Intelligence Brigade (Cyber), a cyber operations technician, and an event coordinator and cadre member for the 4th annual Army Cyber Skills Challenge (ACSC IV), explains a scenario to Staff Sgt. Stanley Brownell during the ACSC IV competition on Fort Meade, October 28. (U.S. Army Photo)

The 780th Military Intelligence (MI) Brigade warrant officers hosted the 4th annual Army Cyber Skills Challenge (ACSC IV) on Oct. 28 to pit 59 participants against one another in order to determine who would be this year's Cyber Champion.

ACSC IV is designed to test participants with a range of physical and technical challenges to highlight how important both physical and technical skills are to today's "Cyber Warrior."

"My intent is to continue the tradition of holding a first class Army "Cyber Warrior" competition to enhance recruiting, foster pride, devotion and honor between the Soldiers and Department of the Army Civilians (DACs) in our burgeoning mission area," said Col. John (Dave) Branch, commander of the 780th MI Brigade.

Soldiers and civilians from across the Army participated in the daylong event. This included representatives from: 1st Information Operations Command, Fort Belvoir, Va.; the 704th MI Brigade, Fort Meade; the Cyber Protection Brigade, Fort Gordon, Ga.; the 82nd Airborne Division, Fort Bragg, N.C., and the 780th MI Brigade, from both forts Meade and Gordon. The participant break out included 50 enlisted Soldiers, three officers and 6 DACs.

According to Chief Warrant Officer 4 Kirk Bond, a cyber operations technician, and one of the 780th MI Brigade event organizers, "This event was created with the intention to challenge participants both physically and mentally, and crown the individual with the highest composite score the ACSC Champion."

"This event was created with the intention to challenge participants both physically and mentally."



Spc. Ryan Roden, Alpha Co., 741st Military Intelligence Battalion, 704th Military Intelligence Brigade, was the 4th annual Army Cyber Skills Challenge Iron Warrior in the physical skills category. Roden beat out 59 other competitors to win the event on Fort Meade, October 28. (U.S. Army Photo)

The physical and technical challenges spanned the spectrum of the Army Warrior Ethos and the "Cyber Warrior" skill sets. The physical events included a modified Army Physical Fitness Test, a 4-mile ruck march with a thirty-five pound rucksack, a modified Army Combat Readiness Test, and a timed run through the United States Marine Corps obstacle course. The technical events included programming, exploitation, forensics, and a crypto-analysis challenge.

"The toughest part of the Cyber Skills challenge is how grueling the physical portion is," said Spc. Dylan Nichols, a cyber operations specialist in Delta Company (Co.), 781st MI Battalion. "It takes so much heart and physical toughness to do these things faster than your opponents. It's something you have to put your all into to win."

Skills Challenge



Spc. Stephen Cosolito (right), Delta Company, 781st Military Intelligence Battalion, was the 4th annual Army Cyber Skills Challenge Cyber Champion in the technical skills category. Cosolito beat out 59 other competitors to win the event on Fort Meade, October 28. (U.S. Army Photo)

Spc. Stephen Cosolito, also a cyber operations specialist in Delta Co., 781st MI Battalion, was the ACSC IV Cyber Champion in the technical category. He felt this year's technical challenge was heavy on digital forensics – specifically Linux file system analysis. Cosolito admitted that while Linux was one of his weaker areas he credits his success to several factors.

“With the competition being timed, my strategy going in was to focus on scoring multiple low point problems early on and then use the remaining time to focus on the higher payoff, more difficult ones,” said Cosolito. “I (also) credit my success to the valuable training I have received as a member of the 781st MI Battalion. I have been afforded the opportunity, time, and funding to attend numerous technical training courses, picking up multiple industry certifications in the process. Beyond this, I have had the luxury of working with some outstanding mentors in the unit and greater enterprise over the past several years.”

Cosolito added, “While I would like to say I did it completely on my own, it would be disingenuous for me to disregard the contributions above that came about through serving in the Armed Forces’ premier CNO (Computer Network Operations) organization.”

The ACSC was introduced in 2013 as a means for the cyber warrant officers to provide a challenging training opportunity for Soldiers and civilians within the

brigade. Since its inception, the event has grown from 11 participants to 59 this year. The event continues to be designed and executed by the warrant officers in the 780th MI Brigade; however, officers and non-commissioned officers have volunteered to help build events and serve as cadre.

“It enables cyber professionals to display their talents by competing against their peers,” said Bond. “Everyone walks away from this event with another tool in their kit. By including a physical portion to the competition, we stress the Total Soldier Concept.”


1st Lt. Christian Sharpsten, a cyber operations officer with Echo Co., 782nd MI Battalion, was the overall Cyber Champion for ACSC IV, and believes it is important to have a cyber skill competition.

“The value of friendly competition cannot be understated,” stated Sharpsten. “The Cyber Skills Challenge provides a way for Soldiers to exercise their unique skillsets and push the boundaries of their own knowledge in a competitive setting. The exhausting physical portion combined with the fast pace of the technical competition emphasized mental agility and the Total Soldier concept. Not only was the Cyber Skills Challenge a tough competition, but also a fantastic learning and self-development experience.”

The 2016 ACSC IV winners were:

- 1st Lt. Sharpsten, Echo Co., 782nd MI Battalion, ACSC IV Cyber Champion (Overall);
- Spc. Cosolito, Delta Co., 781st MI Battalion, ACSC IV Cyber Champion (Technical); and
- Spc. Ryan Roden, Alpha Co., 741st MI Battalion, 704th MI Brigade, ACSC IV Iron Warrior (Physical).

The 780th MI Brigade warrant officers intend to host the ACSC competition in the cloud for future iterations enabling remote sites to compete in real time. Currently, the majority of competitors come from the Military District of Washington area.

Photo Page 

4th Annual Army Cyber Skills Challenge

FORT GEORGE G. MEADE, Maryland –



1st Lt. Christian Sharpsten (right), a cyber operations officer with Echo Company (Co.), 782nd Military Intelligence (MI) Battalion, receives the 4th annual Army Cyber Skills Challenge Cyber Champion trophy from Chief Warrant Officer 5 John O'Reilly (left), technical advisor for the 780th MI Brigade (Cyber), on Fort Meade, October 28. Sharpsten beat out 59 other competitors for the top honor. The event, hosted by the 780th MI Brigade warrant officers, is designed to test participants with a range of physical and technical challenges to highlight how important both physical and technical skills are to today's Cyber Warrior. (U.S. Army Photo)



Sharpsten (left), Spc. Justin Radanovic (center), Delta Co., 781st Military Intelligence (MI) Battalion, and Sgt. Isaias Laureano (right), Delta Co., 782nd MI Battalion, who are both cyber operations specialists, compete in the 4th annual Army Cyber Skills Challenge on Fort Meade, October 28.





Chief Warrant Officer 2 Scott Miller, a cadre member for the 4th annual Army Cyber Skills Challenge (ACSC) gives instructions to participants prior to their 4-mile ruck march on Fort Meade, October 28. Other physical events included a modified Army Physical Fitness Test, a modified Army Combat Readiness Test, and a timed run through the U.S. Marine Corps (USMC) obstacle course. The technical events included programming, exploitation, forensics, and a crypto-analysis challenge. (U.S. Army Photo)



Staff Sgt. Maura Stepanski, Delta Co., 781st Military Intelligence Battalion, took a modified Army Physical Fitness Test as part of the 4th annual Army Cyber Skills Challenge on Fort Meade, October 28. After the competition Stepanski said, "I wanted to challenge myself and finish all obstacles. As a leader I wanted to show Soldiers that you should always push yourself to be better." (U.S. Army Photo)



Capt. Scott Fitzgerald, a Military Intelligence (MI) officer with the 1st Information Operations Command, based out of Fort Belvoir, Va., participates in a timed run through the USMC obstacle course as part of the 4th annual Army Cyber Skills Challenge on Fort Meade, October 28. Other units represented were the 704th MI Brigade, Fort Meade; the Cyber Protection Brigade, Fort Gordon, Ga.; the 82nd Airborne Division, Fort Bragg, N.C., and the 780th MI Brigade, from both forts Meade and Gordon. (U.S. Army Photo)



Chief Warrant Officer 3 Ramon (Ray) Rivera, 780th Military Intelligence (MI) Brigade (Cyber), an event coordinator and cadre member for the 4th annual Army Cyber Skills Challenge (ACSC), discusses the event with Brig. Gen. Maria Barrett, the director, Joint Forces Headquarters-Cyber (U.S. Army Cyber Command), on Fort Meade, October 28. Sgt. Garrett Allen, Echo Co. (sitting in the foreground), 782nd MI Battalion was one of 59 competitors seeking to be this year's ACSC IV Cyber Champion. (U.S. Army Photo)

Partnership between Dutch and Army Cyber Brig

By: Steven Stover, Public Affairs Officer, 780th Military Intelligence Brigade



Col. John (David) Branch (back left), commander, 780th Military Intelligence (MI) Brigade, headquartered at Fort Meade, Md., talks to Brig. Gen. Hans Folmer (back right), commandant of the new Dutch Defence Cyber Command (DCC), to strengthen their partnership and discuss cyber and future training opportunities at the Muscatatuck Urban Training Center (MUTC), March 16. (U.S. Army Photo)

BUTLERVILLE, Indiana – Dutch Brig. Gen. Hans Folmer, commandant of his country's newly-formed Dutch Defence Cyber Command (DCC), met with Col. John (Dave) Branch, commander of the 780th Military Intelligence (MI) Brigade (Cyber), to strengthen their partnership and discuss cyber and future training opportunities at the Muscatatuck Urban Training Center (MUTC) here, March 16.

Folmer was at MUTC to observe how cyber support can enhance tactical operations, in this case, a Dutch Special Operations Forces (SOF) unit in the planning, preparation, and execution of a hostage scenario. The Dutch saw the end state of their BOLD QUEST 17.1 (BQ 17.1) exercise as the identification and experience of how cyber support can assist SOF and the development of SOF unit cyber capabilities.

“Brig. Gen. Folmer is at the early stages of developing his force, and he is developing it in a reverse fashion to how the U.S. did,” said Branch. “Here at Muscatatuck, he is initially looking at it from the tactical piece, but he is the all-encompassing representative to their defense minsters – everything from the tactical to the strategic.”

Last June, Folmer wrote an article entitled “Defense Cyber Command: a New Branch to the Defense Tree.”

In the article, he discusses the current cyber threats, his country's updated Defense Cyber Strategy, and the implementation and organization of the DCC. Folmer believes digital resources are an operational capacity to be used as weapons or an intelligence agent, thus they are an essential part of the operational capability of the armed forces. He considers cyber capabilities as an integral part of military action, including offensive, defensive, and intelligence. Consequently, he sees the DCC's role as ensuring his tactical and strategic-level leadership support the military action with cyber capabilities.

Following an After Action Review for BQ 17.1, Folmer told the Dutch element and Muscatatuck training team that, “One of the directions for the armed forces of the future is we're starting now to develop new units; a new way of (cyber) working with Dutch forces.”

To that end, Folmer and Branch's discussion focused on how the 780th MI Brigade can assist the DCC and its cyber force.

Specifically, they discussed, “How do we train, how we assess our teams in training, and what can we share from a lessons-learned perspective in that set,” said Branch.

Branch compared the tactical training of U.S. cyber teams to what the Dutch were doing in the exercise. Branch remarked that the Dutch MUTC tactical training event parallels closely with what his teams have been learning from the National Training Center rotations in their Cyber Electromagnetic Activities (CEMA) Support to Corps and Below (CSCB) efforts.

“We can share those lessons learned, and there's CALL (Center for Army Lessons Learned) manuals, and then we've invited him to send some of his tactical force to partner with ours and see where we can mesh,” said Branch. “I think that's in the realm of the doable, especially with us, but possibly more so even the Cyber Protection Brigade...given his number one priority is defense of the nation, at least in his early cyber effects.”

Partnering with the U.S. is important to the Dutch

gade Benefits Both Nations



Brig. Gen. Hans Folmer (back), commandant of the new Dutch Defence Cyber Command (DCC), wants to strengthen his country's partnership with the U.S., specifically, in the area of cyberspace training. The Dutch are very interested in the training and certification process for the 780th Military Intelligence Brigade cyber teams. (U.S. Army Photo)

DCC commandant. The Dutch have positioned a liaison officer, Lt. Col. Mark De Wolff, at the Cyber Center of Excellence (CCOE) on Fort Gordon, Ga. De Wolff regularly meets with the cyber units there, to include the 782nd MI Battalion (Cyber). The 782nd is one of two cyber battalions subordinate to the 780th MI Brigade, headquartered at Fort Meade, Md. The 781st MI Battalion is also at Meade.

According to Michael King, the 782nd MI Battalion's Training and Exercise director, the Dutch are very interested in the training and certification process for the battalion's cyber teams.

King's supervisor and the 782nd MI Battalion operations (S3) officer-in-charge, Maj. Tom Nelson, stated, "Mr. King walked him through the T&EO (training and evaluation outlines) manual and we discussed our current 24-month training plan for FOC (Full Operational Capability) VALEX (Validation Exercise), and Recertification MRX (Mission Readiness Exercise)."

Part of the Dutch and U.S. partnership includes sending U.S. cyber Soldiers and civilians to the Netherlands to attend the DCC Cyber Security Insight Course (CSIC). Previously members of the CCOE, the Cyber Protection Brigade (CPB), 780th MI Brigade, 781st and 782nd MI Battalions have attended the course.

"Sending our cyber workforce to the course is a great professional development opportunity and strength-

ens our ties with a coalition partner," said Maj. Deon Singh, 781st MI Battalion S3. "The most valuable part of the course is the knowledge obtained regarding the challenges DCC is having in the cyber realm due to their proximity to EU (European Union) and NATO."

Concisely, the 780th MI Brigade leadership see the true value of the CSIC training is in the relationship building and understanding how a coalition partner is handling the problem everyone is currently facing – security and freedom of operations in the cyberspace domain.

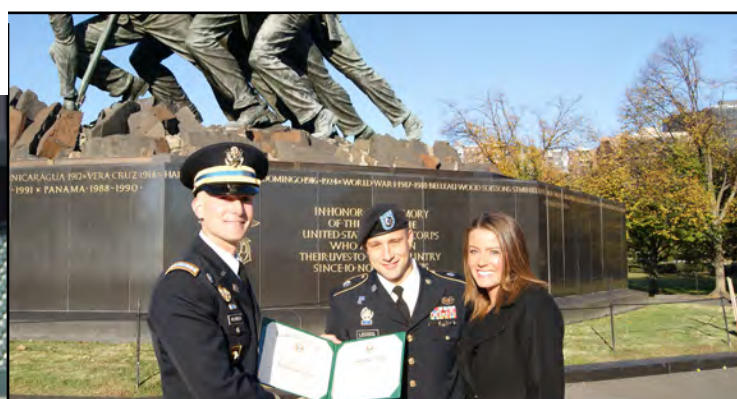
At the end of their meeting Folmer and Branch discussed greater engagement and cooperation in future exercises.

"What's neat to see is folks take this seriously, they understand the impact (cyber) can have, and the importance that they want to assess towards it," said Branch. "I think Brig. Gen. Folmer's at the cusp of building out his force to support both tactical commanders and strategic-level leaders for the Netherlands."



Col. John (David) Branch (left), commander, 780th Military Intelligence (MI) Brigade (Cyber), headquartered at Fort Meade, Md., Lt. Col. Mark De Wolff (center), Dutch liaison officer to the Cyber Center of Excellence, Fort Gordon, Ga., and Lt. Col. David Chang (right), commander, 782nd MI Battalion (Cyber), Fort Gordon, Ga., listen to a Dutch Special Operations Forces (SOF) element discuss cyber support to a SOF tactical exercise in an After Action Review at Muscatatuck Urban Training Center, March 16. (U.S. Army Photo)

Retention



Treat people as they should be treated. In the Soldier's Code, we pledge to "treat others with dignity and respect while expecting others to do the same." Respect is what allows us to appreciate the best in other people. Respect is trusting that all people have done their jobs and fulfilled their duty. And self-respect is a vital ingredient with the Army value of respect, which results from knowing you have put forth your best effort. The Army is one team and each of us has something to contribute.



R
E
T
E
N
T
I
O
N

RESPECT

Hail & Farewell

ANNE ARUNDEL, Maryland -- Seniors leaders from the 780th Military Intelligence (MI) Brigade (Cyber) gathered at Dave & Busters in Arundel Mills Mall, Md., on Mar. 2 to say farewell to several of our senior cyber warriors.



Chief Warrant Officer 4 Raul Negrón, Jr. (left), Cyber Operations Technician, 780th MI Brigade, from June 19, 2013 to February 27, 2017. CW4 Negrón is going to the U.S. Army Cyber School Center of Excellence, Fort Gordon, Ga.



Chief Warrant Officer 5 Craig Jones (right), the Cyber National Mission Force J2 Technical Director, served with the 780 MI Brigade from October 11, 2013 to March 8, 2017. CW5 Jones is heading to the 704th MI Brigade, Fort Meade, Md.



Lt. Col. Brian Davis (right), 780th MI Brigade operations (S3) officer-in-charge, from July 1, 2014 to April 7, 2017. Davis will assume command of the 719th MI Battalion, Republic of Korea.



Lt. Col. David Chang (right), battalion commander, 782nd MI Battalion, served with the 780th MI Brigade from July 22, 2011 to June 2, 2017.

782nd MI Battalion: Leader's week 2017

By: 782nd Military Intelligence Battalion (Cyber)



FORT PULASKI NATIONAL MONUMENT, Georgia – 782nd Military Intelligence (MI) Battalion leadership traveled to Fort Pulaski National Monument for a staff ride as part of their Leaders' Week 2017, the second week in March. The event also included a drone hacking competition, engagements with 3rd Infantry Division (3ID) leadership, and a tour of the Fort Stewart Foundry site. (U.S. Army Photo)

FORT PULASKI NATIONAL MONUMENT, Georgia – 782nd Military Intelligence (MI) Battalion leadership traveled to Fort Stewart, Ga. for a productive Leaders' Week 2017, which included a drone hacking competition, a staff ride at Fort Pulaski, engagements with the 3rd Infantry Division (3ID) leadership, and a tour of the Fort Stewart Foundry site in early March.

The week was a great opportunity for the geographically dispersed battalion to bring the leadership together for some fun events and informative discussion.

Delta Company (Co.), 782nd MI Battalion, led the drone hacking competition where five teams used a laptop and Raspberry Pi to deauthenticate and take control of a flying drone and then navigate it through an obstacle course in the fastest time. The challenge put both the teams' hacking as well as flying skills to the test. 1st Lt. Ian Reynoso and 1st Lt. Benjamin Allison, both cyber operations officers, led their team to victory by being the first to hijack their drone's controls and complete the obstacle course.

The battalion leadership then traveled to Fort Pulaski for a Staff Ride, where Capt. Kevin Jaworski and a National Park Service ranger led discussions on the history of the battle for Fort Pulaski. Focus topics were assigned to each team of leaders to discuss in a small group setting on how a certain aspect of the battle

affected its overall outcome, what lessons were learned and how they apply to today's battlefield in the cyberspace domain.

Col. John (Dave) Branch, commander of the 780th MI Brigade, and Lt. Col. David Chang, commander of the 782nd MI Battalion, and other senior battalion leaders then conducted a strategic engagement and cyber leader professional development with the 3ID commanding general, Maj. Gen. James Rainey, and leaders from the division and brigade combat teams. Branch discussed how cyber forces could support the division and brigade combat teams by protecting and hardening operational networks, improving situational awareness, and conducting cyberspace operations; Jaworski discussed how the 780th MI Brigade's Cyber Electromagnetic Activities (CEMA) Support to Corps and Below (CSCB) detachment is organized and provided an overview of their most recent support to 2nd Armored Brigade Combat Team, 1st Infantry Division at a combat training center rotation; Chief Warrant Officer 3 Jeffery Bisel briefed the targeting process for cyberspace operations and related it to the air tasking order process which maneuver forces already use for conducting air operations; and finally, Capt. Michael Brady reviewed real world examples used by 101st Airborne Division during their recent deployment. These briefings helped to fill the knowledge gap of how to
(Continued on page 26)

Fort Gordon: Unity of Effort

By: 782nd Military Intelligence Battalion (Cyber)



FORT GORDON, Georgia -- Unity of effort in providing joint training opportunities with adjacent military intelligence units here has enabled the Headquarters and Headquarters Company (HHC), 782nd Military Intelligence (MI) Battalion (HHC/782) to grow and develop our low density Military Occupational Specialties (MOS) population.

Collaboration has provided multiple squad-level training events from focusing on Army Warrior Tasks (AWT) to conducting a company field training exercises (FTX) in order to better prepare the unit's administrative, logistics, communications and intelligence Soldiers for NCOES (Noncommissioned Officer Education System) leadership courses, and future assignments within U.S. Army Intelligence and Security Command and U.S. Army Forces Command. More importantly, the unit has been able to promote the cyber branch and provide opportunities for other units here to better understand the application of cyberspace operations at the squad and platoon levels.

HHC/782 and HHC, 297th MI Battalion (HHC/297), part of the 513th MI Brigade, began executing joint training several months ago, mainly focusing on AWT and Soldier-level tasks of vehicle maintenance and establishing radio communications. This developed into an FTX in October where Soldiers were able to practice squad movement, establish a tactical operations center and participate in a shoot house exercise.

The FTX also provided HHC/782 the venue to resource, train and execute a Cyber Electromagnetic Ac-

tivities (CEMA) Support to Corps and Below (CSCB) demonstration of identifying an enemy network and providing real time support to a combatant commander. In this instance, our CSCB Soldiers demonstrated the ability to connect to a wireless camera and provide operational planning input to Soldiers. By demonstrating this capability, HHC/782 Soldiers were able to practice their field craft and demonstrate to others how they effectively support the warfighter.

HHC/782 has also been able to build lines of communication with the Cyber Protection Brigade (CPB). Though it is still in the early stages, HHC/782 has opened lines of dialogue focusing on familiarizing our non-cyber Soldiers and staff on unclassified cyber capabilities. In February, CSCB Soldiers, led by 1st Lt. Stephan Wechsler, a cyber operations officer, and Spc. Justin Longshore, a cyber operations specialist, gave an overview of Kali Linux (a Debian-based Linux distribution aimed at advanced Penetration Testing and Security Auditing) to HHC Soldiers and CPB non-cyber Soldiers. The goal was to achieve cyber familiarization and to increase the knowledge and understanding of cyberspace operations. Because of the value of the instruction, future joint training opportunities are being scheduled between HHC/782, CPB and 513 MI Brigade Soldiers to train on basic Linux command line and increase understanding of the unclassified mission set of the battalion. This opportunity is currently being resourced and developed by one the 782nd MI Battalion's new cyber operations officers, 1st Lt. Andrea Dubin.

Unity of effort between cyber and non-cyber forces is paramount to increase transparency and understanding of the Cyber Mission Force. The battalion's CSCB effort has been able to hone their tradecraft and communication set, and battalion Soldiers have been given the opportunity to train on AWT, NCOES tasks, and prepare for future assignments through building lines of communication with the 513 MI Brigade and the CPB. Ultimately, HHC/782 has set the ground work for continued training of basic cyber operations and capabilities for non-cyber forces and enabled staff to better understand the cyber-warfighter they support.

Proof of Concept – Holistic Cyber Operations Forward

By: Maj. Jason Hogan, commander, Detachment Texas, 782nd Military Intelligence Battalion (Cyber)

SAN ANTONIO -- U.S. Cyber Command executed a proof of concept to test the validity of a Joint Force Headquarters – Forward (JFHQ-FWD), during U.S. European Command's (USEUCOM) recent Tier 1 Exercise, AUSTERE CHALLENGE 17 (AC17) and U.S. Strategic Command's (USSTRATCOM) Tier 1 Exercise, GLOBAL LIGHTNING 17 (GL17). Detachment Texas, 782nd Military Intelligence (MI) Battalion supported these exercises with three planners; two at USEUCOM and one at U.S. Army Europe (USAREUR).

The task and purpose of the JFHQ-FWD is an evolution of the Cyber Support Element concept that proved its worth at U.S. Central Command (USCENTCOM). JFHQ-FWD in essence operates as the cyber component on behalf of the assigned JFHQ-C (Component, i.e. Army, Navy, Air Force, Marines). However, in the future, this element will do more than just offensive cyber planning support. Current recommendations include adding elements from both offensive and defensive cyber teams, including Cyber Protection Teams and National Mission Teams. It is crucially important to provide a holistic cyber operations element in order to fully maximize cyber capabilities and nest with the other domains of land, sea, air and space.

Successful implementation hinges on two main tenants. The JFHQ-FWD must be scalable and flexible to adjust personnel authorizations between different Joint staff (J-staff) sections based on the supported geographic command structure and operations. Secondly, there must be clear delineation in the command and control (C2) execution order between Forward and Main element responsibilities and focus.

During AC17 and GL17, established norms of separating offensive and defensive cyber into different Lines of Operation (LOO) negatively affected situational awareness, intelligence and planning. This separation limited the effectiveness of the JFHQ-FWD. While it is important to have senior leaders at the JFHQ-FWD capable of planning and employing offensive or defensive cyber capabilities, within the

JFHQ-FWD, they must report to the same J-staff lead. For example, within the J-2 (Joint Staff for intelligence) staff, personnel may focus on offense or defense but the JFHQ-FWD J2 would be responsible for all intelligence operations. During AC17 and GL17, that was not executed and was clearly an impediment early on.

De-conflicted and precise LOO must be delineated between the Forward element and the Main. JFHQ-FWD must focus on strategic planning and operations, JFHQ-C must focus on operational intelligence and planning support and the teams must focus on the tactical level. While the JFHQ-FWD can and should be focused on bridging strategic level planning and requirements, JFHQ-C needs to focus on operational intelligence and planning support that is currently lacking to enable tactical cyber operations and planning that the Cyber Mission Teams are currently doing. Failure to deliberately separate the functions by location will severely degrade potential increased capacity for cyber planning and operations through the establishment of a JFHQ-FWD element.

Manpower recommendations from J-1/39/6 (personnel and readiness) and Office of the Under Secretary of Defense for Personnel and Readiness includes organizational structure for staff sections and recommended force allocations. Based on the supported command strengths and command organization, a scalable model for force allocation must be supported. Some staff sections may require less personnel based on the supported command staff strengths and structure. Some of those manning authorizations are better served filling out a small, mission and staff enabling headquarters element and increased J-3 (operations) and J-5 sections (strategies, plans and policy) that include dedicated personnel for component planning support.

Overall, the JFHQ-FWD execution was a success but still limited in the cyber capacity it provided to both USEUCOM and USSTRATCOM. The Forward element streamlined leveraging and integrating the cyber domain forces with other domains. The integration of cyberspace operations was recognized by the (*Continues on the next page*)

(Continued from the previous page)

USEUCOM deputy commander. Similar models, Theater Special Operations Command (TSOC) and others have proven how valuable it is to have a C2 element with the supported command. Finally, the Forward elements will provide another assignment option for the Army if U.S. Army Cyber Command starts to do true talent management. The ability to grow senior leaders at a team and then JFHQ-C, culminating as a planner in the Forward element able to leverage the years of experience at both the tactical and operational levels. The future of cyber operations and our support to geographic Combatant Commands hinges on the successful employment of the JFHQ-FWD.

Leader's week 2017



(Continued from page 23)

employ cyber forces in support of maneuver operations at the division and brigade level. The Fort Stewart Foundry team, led by Duion Ferguson, graciously arranged a rotational Foundry familiarization for the 782nd MI Battalion leadership. The leaders were divided into three groups and were presented with a capabilities brief by the GEOINT (geospatial intelligence) trainer which included a live demo; a tailored brief on J2X support to cyber led by their primary HUMINT (human intelligence) trainer which included a thorough walk-through of information necessary to the Career Management Field for HUMINT reporting and dissemination; and at the third station, leaders were exposed leaders to tactical SIGINT (signal intelligence) through an overview of radio wave propagation. Also, each team built a Yagi antenna which they then tested with a software defined radio to directionally find a local FM radio station.

Overall, the 782nd MI Battalion's Leaders' Week 2017 was a successful opportunity for the battalion leadership to build unit cohesion despite being spread across four states, as well as conduct professional development and spread information about cyberspace operations to the rest of the force.

Joint Build

(Continued from page 14)

"The teams were able to fully integrate across all sub-elements, identify strengths and weaknesses, develop and share processes and best practices, and build relationships. The exercise highlighted areas for sustainment and improvement and demonstrated the value of a joint, integrated team."

"The experience provided the teams with the means to identify their strengths and weaknesses in preparation for their upcoming exercise. The overall concept of this exercise was a good primer to conduct future joint exercises across the CME, and will provide commanders the means to gauge the effectiveness and readiness of their teams," said Sandefer. "Additionally, the opportunity to integrate as a joint team helped bring into context the roles, responsibilities, and functions of the National Mission Team – aspects which are seldom realized during day-to-day operations."

The more robust and challenging brigade scenario helped set up the teams to successfully complete a recent cyber exercise, CYBERKNIGHT. The 780th TREX section and the SDT will look ahead as they continue to work with the other services to outline how they will help to continue to maintain a robust sustainment training program that ensures continued proficiency and readiness of forces to complete the mission.

Spc. Rodolfo Lara, a cyber operations specialist with the 780th Military Intelligence Brigade, briefs senior Army officials, Feb. 28, on operations he conducted as part of an Expeditionary CEMA (Cyber Electromagnetic Activities) Team (ECT) at Fort Riley, Kan. (U.S. Army Photo)



Connective Trust

By: Capt. Shane Sartalamacchia, commander, Headquarters and Headquarters Company, 780th MI Brigade (Cyber)

Unity of effort is the “coordination and cooperation toward common objectives, even if the participants are not necessarily part of the same command or organization, which is the product of successful unified action.” (JP 1) It allows us to achieve objectives that are individually unobtainable. As the cyber domain is vast and extends further than our normal physical terrain, we need to work with the various organizations operating within the cyber domain to be successful. In order to achieve unity of effort, we must continue to build trust with other organizations so that we can operate like a network of networks.

Trust forms the bedrock of any relationship. Since unity of effort depends on relationships, trust is vital to creating it. The 780th Military Intelligence (MI) Brigade (Cyber) has earned the trust of its intelligence and maneuver partners through several of the efforts that we have pushed forward. Dr. Stephen Covey talked about the importance of trust in his book *The Speed of Trust*:

Trust impacts us 24/7, 365 days a year. It undergirds and affects the quality of every relationship, every communication, every work project, every business venture, every effort in which we are engaged. It changes the quality of every present moment and alters the trajectory and outcome of every future moment of our lives – both personally and professionally.

Contrary to what most people believe, trust is not some soft, illusive quality that you either have or you don't; rather, trust is a pragmatic, tangible, actionable asset that you can create – much faster than you probably think possible.”

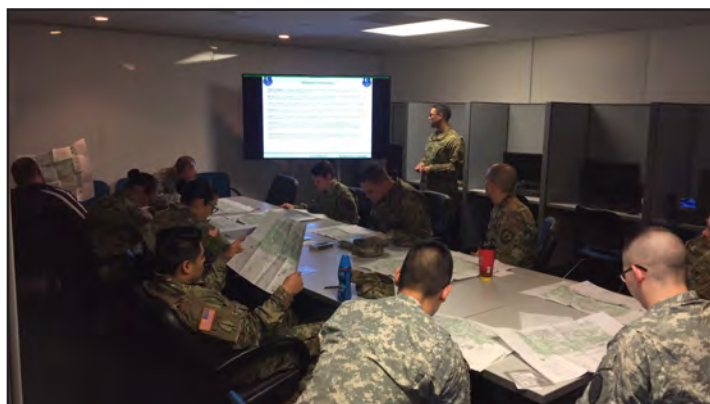
The 780th MI Brigade provides an actualized example of this as the unit that cements the connectivity between the U.S. Army Intelligence and Security Command (INSCOM) and the U.S. Army Cyber Command (ARCYBER). The phrase ‘Intelligence Support to Cyber’ captures the role that the brigade plays in processing, executing, and analyzing the information used to build the targeting framework for offensive cyberspace operations.

Without the trust that enables coordinated freedom of maneuver towards a common goal, we as an organization, ultimately end up excelling in our respective lanes. Actual and literal trust between units in cyber and intelligence is the glue that will enable us to push cyber to the next operationalized level, thereby providing intelligence the information it needs to maintain the situational awareness that the battlefield of the future will require.

Fifteen years of continuous conflict forced disparate organizations and entities to work together to solve common problems; however, with the drawdown in contingency operations, there is less of a demand for the interconnectivity that sustained us in combat. In cyber, where we are in contact with our enemies on a daily basis, that need for unified solutions and flattened organizations creates opportunities for us as intelligence and cyber professionals to maintain the inertia that we nurtured over the last decade.

The 780th MI Brigade is uniquely positioned to bring the Cyber and intelligence communities together in the pursuit of a common goal. Through unity of effort, we enable our brigade and our partners to remain ready at all times. It allows synergy amongst the various intelligence and maneuver organizations so that we may prevail against our adversaries. Unity of effort is what enables our brigade to be “Everywhere and Always...In the Fight.”

Honey Badger 6



Sgt. William Amaro-Fuentes, a cyberspace operations specialist, HHC, 780th MI Brigade, leads Sergeant's Time Training (map reading), in early March. (U.S. Army Photo)

Unity of Effort vs. Unity of Thought

By: Frank Colon, Senior Legal Advisor, 780th MI Brigade (Cyber)



An essential element of success for hundreds of years is unity of effort; however, unity of effort does not preclude the airing and consideration of different views on how to accomplish

the mission. A successful recipe is a robust exchange of ideas prior to finalizing a unity of effort plan. An airing of options, before unity of effort, greatly increases the likelihood that leadership will chose a successful way ahead. However, unity of thought prior to unity of effort can be fatal. NASA Engineers were concerned about the ill-fated “O” rings exposure to cold temperatures prior to launch of the space shuttle Challenger. Tragically, unity of thought cleared the launch and the crew and vehicle were lost. As a result, NASA implemented new measures that facilitate a robust exchange prior to the decision to launch. NASA identified that a unity of thought proceeded the unity of effort resulting in the loss of life and mission failure.

The essential key is timing. Robust discussion occurs prior to the commander’s decision, not in the investigation after. Once the commander has selected the approach, the team must then work together on the way ahead chosen by leadership. Mission risks increase exponentially when members of the team fail to engage in robust discussion prior to a decision or fail to support the chosen course or more seriously, actively disrupt. While the military has disciplinary methods to address individuals who fail to follow orders, the damage to the mission is incalculable. This is true in militaries and democracies.

Unity of effort begins once the leadership selects a way ahead but does not proceed in a vacuum from law and regulation. Once leadership makes a decision, the legal office continues to work with the team as they navigate the challenges of implementation. Just like a unified team, laws and regulations also support unity of effort. Law and regulations exist to provide left and right limits to keep the team from known failure points as the team executes the mission. The left and

right limits established by law and regulation, many times arise out of a prior bad act or in an effort to mitigate unintended consequences. Due to the creativity of humans, not all unintended consequences have been discovered. As a result, just because a law or regulation does not prohibit an act does not make the act permissible. Many times the legal office must extrapolate from existing law or regulation to minimize risks to the command and its mission. Similarly, it is not the responsibility of the legal office to prove an act is prohibited absent specific reference to law or regulation. Absent either express authority or express prohibition, the brigade attorneys make recommendations that keep the brigade efforts in unity with that of the Army, the Department of Defense and our missions.

We are subject to a dizzying array of law and regulation many of which do not directly apply to cyber operations requiring interpretation. Additionally, our mission is inherently complex and has the potential to create effects beyond our command and nation. The role of the legal office is to resolve interpretation issues arising out of law and regulation. The combination of our complex mission and nascent law and regulation demand unity of effort for mission success. The legal office supports the brigade and commander to ensure unity of effort with our daily operations and support to successful global cyber operations.



Together We Can Combat Sexual Harassment and Assault

By: Kimberly Henne, Sexual Assault Response Coordinator, 780th MI Brigade (Cyber)

The theme of this edition of “The Byte” is unity of effort. Webster’s definition is “the state of being united or joined as a whole.” A synonym of unity is homogeneity. The Army is composed of many individuals from a variety of locations, backgrounds, and life experiences. Certainly not the definition of homogeneity. The only characteristic that makes the Army homogeneous is our humanity; however, the Army Values: Loyalty, Duty, Respect, Selfless Service, Honor, Integrity, and Personal Courage, lend to creating that homogeneity throughout our force of Soldiers, civilians and contractors.

The Army recruits its Soldiers from the society at large – from different locations and cultures. Once these Soldiers enter into the service they are expected to immediately live the Army Values; however, due to their upbringing, they may not actually know what those Army Values stand for or what behaviors run contrary to those Values. It is a learning process for new recruits to learn the meaning of our Army Values, and it is all our responsibility, working together, to teach our

young Soldiers what is acceptable behavior within the realm of dignity and respect for all.

The Brigade SHARP Team (Sexual Harassment/Assault Response & Prevention) works with our counterparts at every installation where we have subordinate units, working on prevention and response for our team members who live and work in those areas. These include: Schofield Barracks, Hawaii, Joint Base San Antonio-Fort Sam Houston, as well as with the Fort Gordon, Ga., and Fort Meade SHARP Teams. We also work with the other Major Subordinate Commands, such as the 704th Military Intelligence (MI) Brigade and 902nd MI Group, on Fort Meade, the 500th MI Brigade in Hawaii, the 470th MI Brigade in Texas, and the 116th MI Brigade at Fort Gordon. By working together, we create prevention programs and we ensure all our team members receive the services they need.

Newly included in receiving those SHARP services are Department of the Army Civilians (DAC). DACs can now receive a RESTRICTED Report of sexual assault from the SHARP Program. That means a DAC who has been assaulted can get assistance and referrals from the SHARP Team without their supervisor or the command team ever knowing about the assault.

So, another phrase meaning Unity of Effort can be “working together.” It takes all of us – Soldiers, DACs, and Contractors working together to combat sexual harassment and sexual assault within our ranks.

If you would like to speak with a member of the SHARP Team, please call 301.833.6407 or 24/7 410.693.4638. You can also speak with someone confidentially at the DOD Safe Helpline at 877.995.5247.



April is Sexual Assault Awareness and Prevention Month and the 780th Military Intelligence Brigade Soldiers and Army civilians started the commemoration with a pledge signing event in front of the brigade headquarters, April 5. Pictured here are the brigade’s SHARP team (from left to right) Sgt. 1st Class Noe Depriest, Sgt. 1st Class David Strohacker, Staff Sgt. Sean Loveridge, Kimberly Henne, SARC, Sgt. 1st Class Tammy Cross, brigade Victim Advocate, Staff Sgt. Brandilyn Corn-tassel, Staff Sgt. MarQuita Lacey, and Sgt. 1st Class Robert Fitzwater. (U.S. Army Photo)



Army Diversity: Strength in Diversity

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

In January, our country celebrated the life and accomplishments of Dr. Martin Luther King Jr., a Baptist minister and activist, who was a leader during the Civil Rights Movement. The Fort Meade observance took place on Jan. 19, with guest speaker, Mr. Robert Ewell Greene, and the event included a performance by the Largo High School choir, from Upper Marlboro, Md.

These monthly Fort Meade Equal Opportunity (EO) observances are always a great place to explore and learn about our nation's diverse culture and history.

The monthly EO observances have been a great success; however, they cannot be accomplished by any one entity or organization. They are accomplished through a unity of effort between the military units on post, local community organizations and schools, Army Community Service (ACS), Morale Welfare and Recreation (MWR), as well as many other people and organizations. Equal Opportunity Advisors (EOAs) from units across the post come together for 10 observances annually to ensure Soldiers, civilians, and family members are able to celebrate and honor - to remember - the diverse groups of people that make up our country's culture and society.

The EOAs' support to their units is no different. We work hand-in-hand with each other to ensure the Equal Opportunity Leaders (EOLs) are trained correctly and efficiently during the quarterly Equal Opportunity Leader Course (EOLC). Each quarter Soldiers with the rank from Sgt. (promotable) through 1st Lt. attend the EOLC, trained by EOAs from units all around the Military District of Washington, including Fort Meade, Fort



Display from January 2017 MLK Observance

Belvoir, Va., and Joint Base Myer-Henderson Hall, Va.

As members of a diverse workforce, comprised of people from around the country and various parts of the world, it is important that we maintain a unity of effort in our everyday work ethic. Treating each member of the team with dignity, fairness, and respect is how we can best achieve the spirit of unity of effort. The mission of the Brigade EOA is to support every member of the 780th MI Brigade team, and I will ensure that I coordinate and work with every element necessary in order to accomplish that mission.

If you need to reach of me, call 301.833.6412 (work), 301.974.2763 (cell), or email me at eric.d.frock.mil@mail.mil. If I do not answer, please leave a message, and I will get back to you as soon as I can. If you need to see me in person, I am in the Annex trailer at 310 Chamberlin Ave. on Fort Meade, Md. Additionally, you can contact your unit's Equal Opportunity Leader for assistance.



Resilience: How applying Army resiliency in you

By: Sgt. 1st Class Kalen Phillips, 781st Military Intelligence Battalion (Cyber)



1st Lt. Alvaro Luna (standing), explains the brigade-level operations that will occur during the next National Training Center rotation and how cyber effects will be integrated into them. Spc. Paul Estipona (sitting to his left), is part of the Cyber Electromagnetic Activities (CEMA) Support to Corps and Below (CSCB) section. (U.S. Army Photo)

Spec. Paul Estipona was born and raised in Manila, Philippines. After completing high school, Estipona attended De La Salle University where he received his Bachelors of Science degree in Civil Engineering, majoring in Construction Management. He decided to make the move to America to practice his Civil Engineering profession and help support his family. After working as a construction estimator and AutoCAD draftsman, Estipona decided to join the U.S. Army because he always wanted to be in the Service and was drawn by the history and tradition of the Army. After completing both basic and advanced individual training, Estipona's specialty was a helicopter repairer, and he was initially assigned to the Combat Aviation Brigade, 4th Infantry Division as a UH-60 Blackhawk mechanic in late 2013.

"Aside from being a premier fighting force, I saw in the U.S. Army that it can also be a beacon to promote peace and order and the right ideals for a good cause. That is why I was always drawn to join the Army."

In the fall of 2014, Estipona applied to become a commissioned officer in the Army through the Green to Gold program. This drive came from his desire to continue his selfless service in the Army profession where he had social unity and cohesion. He received a medical screening as part of his application and was informed by his primary care manager that his White Blood Cell (WBC) count was alarmingly high. Based on the screening results, Estipona underwent multiple follow on examinations and after review by Pathologists at Evans Army Community Hospital at Fort Carson, Colo., he was diagnosed with Stage IV-B Hodgkin's Lymphoma in November 2014.

"After being diagnosed with Lymphoma, my whole world felt like it came crashing down. All my hopes and dreams were put on hold and it seemed like it was the first time I couldn't control where my life was headed."

Estipona received six cycles chemotherapy from Nov. 2014 to Apr. 2015. Following chemotherapy, Estipona underwent a PET-CT Scan in June 2015 and was declared to be in remission by his primary Oncologist.

"The first line of treatment was a success, and I attributed my strength and determination from my faith in God, whom I knew would never leave me abandoned or hopeless."

As part of his recovery, Estipona was assigned to the Warrior Transition Unit at Fort Carson, in January 2015. During this period he received full treatment for his medical condition and rehabilitation. After successfully completing both, he went to the medical board in June 2016 and was determined to be fit for duty and approved to re-class to his new specialty as a cyber operations specialist. Estipona went through the Joint Cyber Analysis Course (JCAC) at Pensacola, Fla. where he successfully completed the course with honors and graduated on July 28, 2016.

"I had a totally new perspective about life. To me each moment was a gift from God and being alive each day and having survived cancer was such a great blessing. I made a promise to myself to make the most of each day I lived and every moment I had."

ur life can help you overcome any life challenge



Sp. Paul Estipona, and his wife, Susan Sia, at the 780th MI Brigade Holiday Ball, December 2, 2016. (U.S. Army Photo)

After completing JCAC in Pensacola, Fla., Estipona was assigned to 781st Military Intelligence (MI) Battalion, Fort Meade, Md. After arriving to the unit in Sept. 2016, Estipona again felt some back pain again and the symptoms continued to progress. After a few weeks of continuous pain, Estipona checked himself into the Emergency Room at John Hopkins Hospital in October 2016.

After careful review by the pathologists at Walter Reed, they determined that the developing mass that was causing the pain was a relapse of the Hodgkin's Lymphoma.

"It seemed like I was back where I started again. But I knew I couldn't give up at this point. All I knew was that I needed to push myself again and dig deep again and knew every ounce of strength would be needed from me"

After his diagnosis, Estipona immediately received three cycles of Reinduction Chemotherapy. After his third cycle, Estipona received a follow on PET-CT scan to see if the Hodgkin's Lymphoma had responded

to the treatment. In late Dec. 2016, Estipona received the results of his PET-CT scan identifying him to be again in remission.

"Beating cancer a second time around felt like fighting a very long war. But again I knew giving up was not an option. I cannot stop, because a lot of people - my family, peers and unit - were helping me get through."

For now, the treatment is complete and the cancer is in remission.

"All I could think about at this point are better times, and what could come over the horizon, once all my treatments are over. Which means being with my family, spending time with my loved ones, being able to run again, work-out, be healthy and most of all be in the profession I always wanted to be which is being a cyber operations specialist back in my unit, contributing to the overall mission and working with my peers and command."

SPC Estipona looks forward to attending the sergeant promotion board and is currently studying so he can take on new leadership challenges in the 780th MI Brigade (Cyber).

"My goal, other than to be the best Soldier or NCO (non-commissioned officer) I can be, is to be able to extend and offer the same help and support I received - all this time - from my seniors during my most difficult times, and return the gesture to my peers and subordinates when it is my time to lead."



Sp. Paul Estipona (pictured fourth from the right), and the 780th CSCB section. (U.S. Army Photo)

Resilience: Overcoming Challenges

By: Chaplain (Maj.) Gregory McVey, chaplain, 780th Military Intelligence Brigade (Cyber)



Physical fitness is not the only hallmark of the U.S. Army. Resiliency also ranks high in developing strong Soldiers, Army civilians and Families. Resiliency is defined as trauma, tragedy, personal crises, everyday life problems, with the ability to bounce back stronger, wiser, and more personally powerful. One of several methods to assist in overcoming life's challenges is to manage and control our thoughts.

Marcus Aurelius, Roman Emperor from 161 to 180 A.D., stated, "The most important things in life are the thoughts you choose to think." If this is true, then one of the most important decisions you and I will make today is what to think about.

We can think thoughts of faith or thoughts of doubt, thoughts of hope or thoughts of despair, thoughts of love or thoughts of hate. These thoughts will find their way into our words and our actions as the day wears on.

"Thoughts should be tested before they're transmitted," said the late William Arthur Ward. Ward was a motivational speaker, author, and served in the Army during WWII. He went on to say, "If our thoughts taste unkind, critical or unfair, we should refuse to release them into the dangerous world of words."

Every temptation begins with a thought. So does every act of goodness. The Apostle Paul said in Romans 12:2, "Let God transform you into a new person by changing the way you think."

Today, put resiliency at the top of your "To Do" list, by managing your thought life. Let thoughts of faith, hope and love fill your mind. Make a choice to believe the best about the future God has planned for you. That's faith. Make a choice to expect the best in each situation, because God is at work in the details. That's hope. Make a choice to give the best to those around you, because this is what He has called you to. That's love.

Your resiliency can be measured by the thoughts you think, and the life those thoughts inspire.



Staff Sgt. Daniel Collazo (right), a signal intelligence analyst, reenlisted at Camden Yards, the Baltimore Orioles ballpark, on March 29. Collazo was accompanied on the field by his wife (center), Andrea King. The reenlistment officer was Capt. Shane Sartalamacchia (left), commander, Headquarters and Headquarters Company, 780th Military Intelligence Brigade -- Staff Sgt. Anthony Myers (far left) is holding the U.S. Flag. (U.S. Army Photo)

781st MI Battalion Run



Lt. Col. Justin Considine, commander, 781st Military Intelligence Battalion, leads his organization on a four-mile run here, April 7. (U.S. Army Photo)

Soldiers Become NCOs and Members of a Time Honored Corps

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

No one is more professional than I. I am a noncommissioned officer, a leader of Soldiers. As a noncommissioned officer, I realize that I am a member of a time honored corps, which is known as "The Backbone of the Army..."

FORT GEORGE G. MEADE, Maryland -- 31 Soldiers joined the noncommissioned officer (NCO) ranks in an NCO induction ceremony hosted by the 781st Military Intelligence (MI) Battalion in the McGill Ballroom here, April 11.

Command Sgt. Maj. Brian Cullen, the garrison command sergeant major for Fort George G. Meade, was the guest speaker and part of the official party. Other members of the official party were Command Sgt. Maj. Cecil Reynolds, 781st MI Battalion (Cyber), and 1st Sgt. Stanley Collins, Echo Company (Co.), 782nd MI Battalion (E/782).

Prior to ceremony Cullen explained the importance and separation that occurs when a Soldier becomes an NCO.

"It's a challenge because NCOs, as they get promoted, are still with the Soldiers with whom they serve," said Cullen. "After the ceremony, it shows that separation has now occurred, and they are now leaders of that organization."

The ceremony was steeped in Army tradition and included an acapella singing of our National Anthem by Spc. Manning Stone and an invocation by Staff Sgt. Daniel Goodman. Members of the 781st MI Battalion read the history of the NCO Corp and NCO Creed, and the recitation of the NCO Creed was presented by 1st Sgt. Danny Hurst, Alpha Co., 781 MI Battalion (A/781), Master Sgt. Cory MacNeil, Delta Co., 781 MI Battalion (D/781), and Sgt. 1st Class David Jorden, Charlie Co. 781 MI Battalion (C/781).

After being officially inducted into NCO Corps and

receiving a copy of the NCO Creed and the NCO Charge from the official party, the newly minted NCOs recited the Oath of the United States Army NCO and the Charge of the NCO.

Following the ceremony, Sgt. Garth Summey, D/781, one of the new NCOs, discussed what the ceremony meant to him and his goals for the future.

"Being an NCO means much more responsibility," said Summey. "I need to be an example and take into consideration other people's needs, more so than I did when I was a lower enlisted."

Summey said that while his long-term goal was for more advancement; his focus at this point was on becoming an expert in his field.

Cullen had this advice for the new NCOs, "Be patient, never stop learning, and always ask questions. And most of all, take care of your Soldiers. Take care of them and they'll take care of you."



Participating in ceremony and joining the NCO Corps were – Sgt. Benjamin Allen, B/781; Sgt. Jonathan Baker, D/781; Sgt. Daniel Cardinale, B/781; Sgt. Michael Chong, B/781; Sgt. Taylor Domschke, D/781; Sgt. Gregory Esquivel, B/781; Sgt. James Fearing, A/781; Sgt. Reed Follensbee, C/781; Sgt. Joshua Gallamore, A/781; Sgt. Derek Gilbert, D/781; Sgt. Daniel Goodman, E/782; Sgt. David Gunnerson, E/782; Sgt. Jeffrey Lu, D/781; Sgt. Melanie Miller, C/781; Sgt. Michael Morin, B/781; Sgt. Moriah Moya, A/781; Sgt. Christopher Pandoliano, D/781; Sgt. Jason Postema, C/781; Sgt. Justin Riopelle, E/782; Sgt. Kristina Robertson, E/782; Sgt. Andrew Sessoms, B/781; Sgt. Brian Stout, E/782; Sgt. Garth Summey, D/781; Sgt. Cameron Sutherland, E/782; Sgt. Ryan Szaroletta, A/781; Sgt. Aisha Umar, C/781; Sgt. Ryan Vandegriff, B/781; Sgt. Jesus Vargas, D/781; Sgt. Gregory Waxmonsky, D/781; Sgt. Stewart Williams, B/781; and Sgt. Allyn Wilson, A/781.



Soldiers Lead and Mentor Local High School to Cyber

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



WAHIAWA, HAWAII – Soldiers from Detachment-Hawaii, 782nd Military Intelligence Battalion, mentor Leilehua High School JROTC cadets who are participating in the school's CyberPatriot program. Pictured standing are Chief Warrant Officer 3 Lee Unrein (left) and Sgt. Matthew Meador (right), and sitting (from left to right) Cadets Jarod Olive-Stalling Jr., Brandon Unrein, and Jacob Huerta, and Spc. Evan Wittman. (U.S. Army Photo)

BALTIMORE – Soldiers from Detachment Hawaii (DET HI), 782nd Military Intelligence (MI) Battalion, mentored and led a high school team to the CyberPatriot IX, National Finals Competition, at Baltimore's Hyatt Regency, April 3 to 5.

Although the Leilehua High School CyberPatriot team from Wahiawa, Hawaii, did not finish in the top three in their All Service division, according to Bernie Skoch, the CyberPatriot national commissioner, an NCAA team has a better chance of reaching the Final Four than a high school CyberPatriot team does of reaching the CyberPatriot National Finals.

"The biggest sporting event over the past couple months has been the March Madness...NCAA Basketball Tournament, and given the size of the field, for women or for men, the probability of a team reaching the Final Four is about 1.2 percent," said Skoch. "We had 4,404 (teams) when we started this season. We are down to 28. The probability of a team being here tonight is not 1.2 percent, it's 0.6 percent."

The team's name and school mascot, is the "Mules," and consisted of CyberPatriot members and Junior Reserve

Officer Training Corps' cadets: Tyler McWilliams, ninth Grade, Jacob Huerta, 10th Grade, Jarod Olive-Stalling Jr., 10th Grade, and Brandon Unrein, 12th Grade. The team's coach is retired Army Lt. Col. Nick Spiridigliozzi, the Leilehua High School JROTC senior instructor.

"If it wasn't for the mentors, we wouldn't have made it this far," said Olive-Stalling. "Everything we do, we're going to do in the future."

The Soldiers from 782nd Detachment-Hawaii, have been mentoring high school students to compete in the Air Force Association's CyberPatriot program since the 2015-2016 school year.

Spc. Evan Wittman is the lead mentor, and although other DET HI cyberspace Soldiers have volunteered their time, after work and on weekends, to mentor the students, due to funding and other mission requirements, he was joined in Baltimore by Chief Warrant Officer 3 (CW3) Lee Unrein, father of Cadet Unrein, and Spc. Jacob Cochran.

"The youth are our future leaders and problem solvers. Developing students' interest in STEM (Science, Technology, Engineering, Mathematics) will pay dividends for our Service, Corps and nation," said CW3 Unrein. "Watching the cadets and my son learn and grow has been very rewarding."

Although being a CyberPatriot team member has its benefits, there is also a tremendous amount of research and studying, above and beyond the student's regular class work.

"They give us extra work, besides our homework, so when we come to practice we really know what we're talking about," said Huerta. "Without them, we probably wouldn't be here, so we're really appreciative."

During the CyberPatriot IX, National Finals Competition, each student was able to use what they were taught by their mentors.

"My mentor, Wittman, he really helped me out with networking...You have to know a lot of commands, so during the competition, I was able to go through routers and switches and set them up perfectly so it worked for everybody," said Cadet Huerta.

Patriot National Finals

"I've had three mentors teach me about Linux: Spc. (Joshua) Abraham, Spc. Cochran, and 1st Lt. (Benjamin) Allison," said Cadet McWilliams. "They taught me system development from Unix, and Man Commands that I can use to defend a system running on Linux."

"The mentors make sure we understand it, and push us to keep trying and learning," added Cadet Unrein. "I used Wireshark to trace all the traffic that comes over the computer. It keeps a massive log of every packet that goes through and it can tell you what people tried to do, where they came from, the IP (Internet Protocol) address...it's a way to figure out if someone was trying to connect when they weren't supposed to."

Spc. Cochran encourages other Soldiers to support the program. He had fun mentoring the students, but more importantly, he feels he made a difference in their lives by helping them further their education and prepare for the future.

"I enjoy working with the kids. I love seeing that light when they get it and they start connecting it," said Cochran. "When I was at their age, I didn't know nearly as much as they do now."

In addition to the mentor training, each CyberPatriot student gets a NetAcad (Network Academy) account sponsored by Cisco. They have access to various training modules that teach: network fundamentals, switch and router basics, access control lists, firewalls, Adaptive Security Appliance (a Cisco program), the Internet of Things, and Linux basics. Once students complete the courses, Cisco presents them with a certificate of completion. According to the mentors, the certificates will look good on a student's resume and provide them with an advantage over their peers.

"It does help them go out and get a CCNA (Cisco Certified Network Associate) certificate," said Unrein. "It'd be very interesting to see how the curriculum at our school houses compare to what the cadets receive in the CyberPatriot program."

Though this season was the CyberPatriot program's ninth year, event organizers hope to expand the program.

"We high-five this year with 4,404 teams," said Skoch. "(However) there are 34,000 high schools in the United States, and an equal number of middle schools."

The 780th Military Intelligence Brigade hopes to expand their support as well.

"There's an opportunity, given the geographic dispersion of the 780th Military Intelligence Brigade, to expand our partnership with our local communities and the high school JROTC CyberPatriot programs," said Lt. Col. Chris Longo, deputy commander, 780 MI Brigade. "We have elements, not only in Hawaii, but in San Antonio, Augusta, Georgia, and here at Fort Meade, Maryland."

Although Cadet Unrein will graduate from Leilehua High School later this year, and plans to study cybersecurity at either Towson University in Maryland, or the University of Hawaii at Manoa, the other three cadets, with their mentors help, expect to return to the CyberPatriot National Finals competition next year...and their mentors are already planning for it.

"Next year we'll definitely do more packet analysis with Wireshark, forensics, steganography," said Unrein. "I would also train the students on scripting and programming. Start developing that young. It better prepares them for college. In fact, high schools offer Java programming, CCNA (Cisco Certified Network Associate)...it's really amazing what they offer to the kids now days."



BALTIMORE – The Leilehua High School CyberPatriot team, their coach and mentors: Standing (from left to right), Cadet Tyler McWilliams, Chief Warrant Officer 3 Lee Unrein, Cadets Brandon Unrein and Jarod Olive-Stalling, Spc. Jacob Cochran, and Spc. Evan Wittman. Kneeling are retired Lt. Col. Nick Spiridigliozzi (left), the team coach and JROTC senior instructor, and Cadet Jacob Huerta. McWilliams, Huerta and Unrein aspire to be cyber defense professionals for the National Security Agency, and Olive-Stallings wants to be a Naval Officer after graduating from high school. (U.S. Army Photo)

FORT GEORGE G. MEADE, Maryland - Army Spc. Dylan Nichols, a cyber operations specialist with Delta Company, 781st Military Intelligence Battalion, participates in a timed run through the U.S. Marine Corps obstacle course as part of the 4th annual Army Cyber Skills Challenge on Fort Meade, October 28. (U.S. Army Photo)

