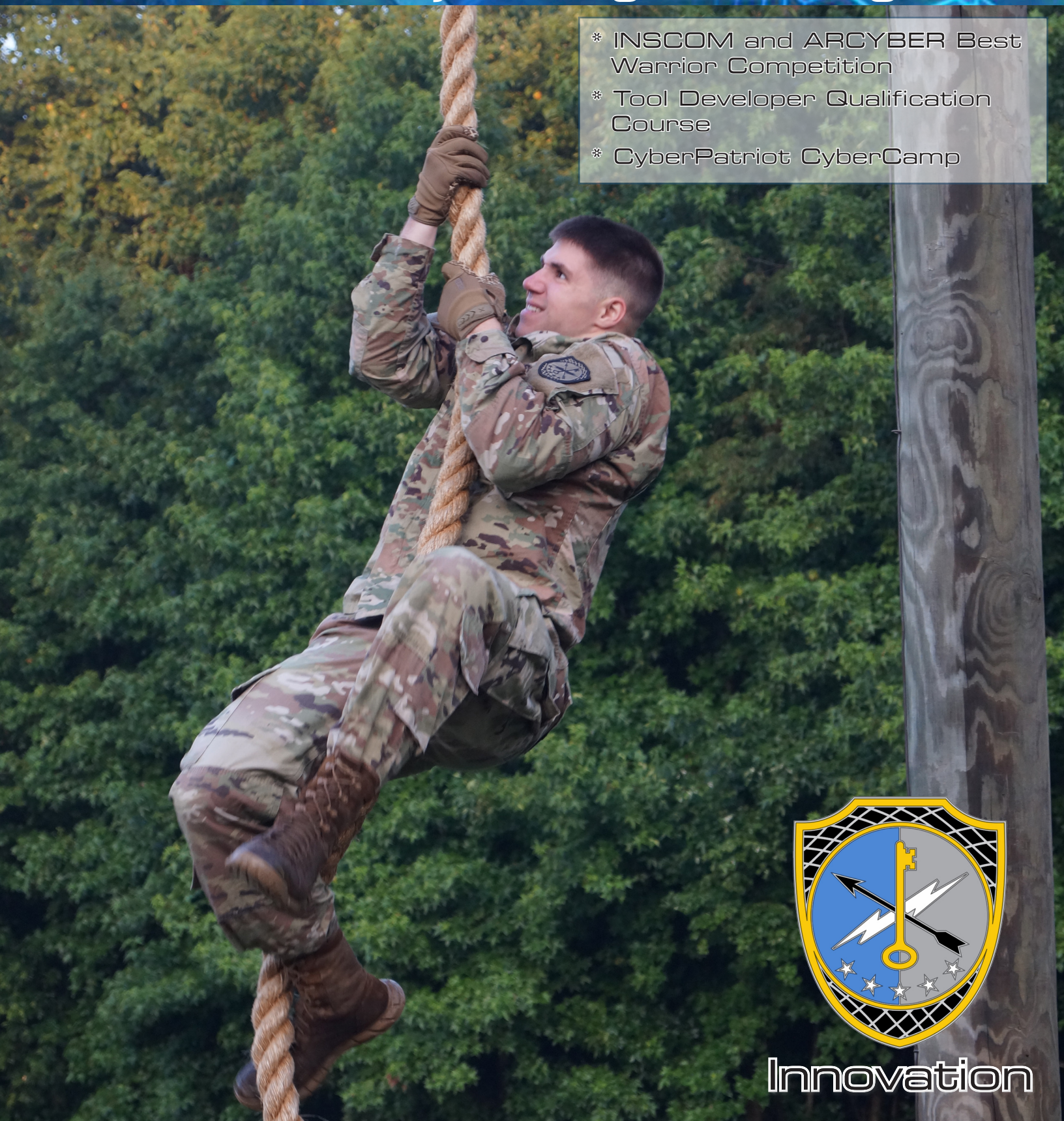
Volume 7, Issue 2

the BYTE

780th Military Intelligence Brigade



* INSCOM and ARCYBER Best Warrior Competition
* Tool Developer Qualification Course
* CyberPatriot CyberCamp

Innovation

PRAETORIANS

780th MI BDE

"STRENGTH AND HONOR"

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

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

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

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

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

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

Col. Brian D. Vile
Commander

Command Sgt. Maj. James M. Krog
Command Sergeant Major

Steven P. Stover
Public Affairs Officer
and Editor

Columns

In every issue...

Photos

Odenton Regional Library Hackathon: A free STEM event for teenagers hosted by the Anne Arundel County Public Library and the 780th Military Intelligence Brigade from 4 to 7:30 p.m. on September 10, October 8, and November 12 (pg. 42).

On the cover:

QUANTICO, Va. -- Sgt. Kyle Tamraz of the 781st Military Intelligence Battalion, 780th MI Brigade (Cyber) tackles the obstacle course event during the U.S. Army Cyber Command (ARCYBER) Best Warrior Competition, at Marine Corps Base Quantico, Va., July 24. (Photo by Bill Roche, ARCYBER)

Features

Articles

From the Editor

The theme for this issue of the BYTE is "*Innovation*".

The U.S. Army Operating Concept defines innovation as "the result of critical and creative thinking" and "the conversion of new ideas into valued outcomes."

The Brigade Vision Statement states "We are America's most innovative cyberspace operations force, deterring, and when directed, defeating our nation's adversaries in and through cyberspace."

In this issue of the BYTE we asked our contributors to apply innovation to the cyberspace domain and electromagnetic spectrum, e.g. how leaders stimulate innovation, persistent innovation, historical examples of innovative success (bombing from aircraft, WWII and Iraq Rhino, the Ho Chi Minh trail) and/or innovative fails (missiles vs. guns on aircraft, Schweinfurt ball bearings, British Strategic bombing theory) – relying on legacy technologies or failing to meet operational requirements -- deliberate versus a hasty attack and how this combat arms tactic could apply to cyber; innovation and the serenity prayer.

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

v/r,
Steve Stover

Public Affairs Officer
780th MI Brigade
Editor, the BYTE

the BYTE: INSCOM's nominee for the 2018 Maj. Gen. Keith L. Ware Public Affairs Competition. The annual Department of Army's competition recognizes Soldiers and DA Civilians for excellence in achieving the objectives of the Public Affairs Program.

'80MIB QRCode.png

Praetorian 6: Leaders Enable Innovation

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

Success in military operations requires innovation, seeking new and novel ways to solve problems. This is especially true for cyberspace operations; our domain changes too frequently and is too complex to expect success without innovation. Yesterday's tools and techniques will rarely be successful - we are often one patch or one firewall modification away from losing years of work. For the Brigade to be successful, every Soldier and Civilian must be empowered to innovate, and leaders must enable them by assuming the associated prudent risk. Wherever we see innovation, we must recognize it, encourage it, and spur it on. Innovation isn't just a buzzword; it is mission critical task that all team members must embrace, promote, and reinforce.

Every Soldier and Civilian must be empowered to innovate, and leaders must enable them

The requirement for innovation is not a new concept nor one unfamiliar to our Soldiers; battlefield innovation has always been a hallmark of U.S. military action on the battlefield. Although there are countless vignettes of American innovation, the story of Culin's Rhino is particularly informative.

Following the invasion of Normandy in 1944, U.S. Soldiers were confronted by a challenging German defense that effectively utilized the local terrain to their advantage. Hedgerows, piles of dirt, rocks, and shrubbery that French farmers had built up over years of improving their fields, provided ready-made defensive positions. In addition to facing German soldiers dug into these ready-made defensive positions, the hedgerows limited armored movement. Making a bad situation even worse, tanks were forced to show their light belly armor to German anti-tank weapons even if they could surmount the obstacles. The fighting was intense, progress was slow, and casualties ran high.

While discussing the deadly challenges they faced, a Soldier named Roberts joked about putting teeth on the front of their tanks to cut through the hedges. While others laughed, an innovative non-commissioned officer, Sergeant Curtis G. Culin, heard the comment and realized there may be a way to make it work. Utilizing steel from German obstacles intended to destroy Allied landing craft, he welded steel horns to the front of a tank. This simple modification allowed the tank to drive through a hedgerow rather than over it, and enabled Allied forces to effectively maneuver against and through the German defenses. Sergeant Culin's innovation, nicknamed the Rhino Device, was quickly adopted across the front line. Maneuver was restored, Allied lives were saved, and the inevitable march to victory was quickened.

When faced with a challenge, Sergeant Culin innovated. He didn't document his requirements, send them to a program manager, and wait for an overpriced and ineffective capability. He saw a solution, executed it, and was met with success. His leadership didn't ask for permission from the Ordnance Department back in the U.S. before modifying their tanks; they assumed the minimal risk associated with the change to enable success on the battlefield. Years later, President Eisenhower remarked on how notable this risk assumption was; "Because this seemed like a crazy idea, they did not even go to the engineers very fast because they were afraid of the technical advice…" 75 years later, you can still imagine a staff officer stifling innovation due to concerns over voiding the tank's warranty.

Instead, Sergeant Culin's innovative spirit was empowered by his chain of command. Upon seeing the invention, General Bradley ordered hundreds

Continued on page 3

Praetorian 7: Innovative Thinkers

By Command Sgt. Major James Krog, Senior Enlisted Leader, 780th Military Intelligence Brigade (Cyber)

This quarter's newsletter topic of innovation has a lot of meaning for me. In my 33 years of service in the Army, I have seen a lot of innovation across the Army. While there continues to be a lot of "if it isn't broke, don't fix it," innovation has played an even greater role. When I joined the Army, engineers built bridges by hand, pickup trucks and deuce and a half trucks were the major mode of transportation for the Army, basic training units used cattle trucks to move Soldiers, audio transcriptions were done using cassette or reel to reel recordings, computers were new, and cell phones did not exist. Today, we have vehicles that lay bridges for us, MRAPs and 5-ton trucks are the major modes of transportation, audio transcriptions are performed using digitized audio, and almost everyone has access to a computer and a cell phone. The Army is constantly innovating to increase the survivability of its greatest resource, its Soldiers, during conflict. Innovation though is not just new equipment, it is also thinking outside the box for ideas on how to use current equipment in new ways or how to improve planning to better accomplish the mission.

Not all innovation, however, fully meets what it is intended to do. One must use caution when implementing innovative ideas to ensure that they meet their full intent without leaving something undone. For example, it may be hard to believe, but I did not send my first text message until my second deployment to Iraq in 2007. Sure my two oldest daughters were text messaging pros, but it was a new concept to me. It is a way of getting information out to the masses, but a text sent isn't necessarily a text read. Leaders must be cautious in using this as a sole method of communication. Follow up is required to ensure the information has reached its intended audience. Too often this follow up is not conducted and information is lost or a required action is not completed. Even today I am not a great fan of text messaging as I much prefer face to face interaction, but it is a major method of communications in today's society.

The Army has obtained some of the best equipment for protecting its Soldiers. The armored HMMWV, the MRAP, and the Improved Outer Tactical Vest are all items that have improved the survivability of Soldiers. Digital systems for collecting and storing data are improving faster than the Army's acquisition community can purchase them. It has also obtained equipment to better enable Soldiers to accomplish their missions. I had the pleasure of being stationed and deployed with some very innovative Soldiers while assigned to the 10th Mountain Division at Fort Drum. The first half of my deployment to Baghdad in 2005, we were successful, but it was slow going. Two of my Soldiers collaborated to write a couple of Microsoft Excel macros that enabled the team to process and analyze large amounts of data in one-tenth the time it normally took us. Additionally, in January 2006, the Army issued the platoon some improved targeting equipment provided a limited amount of training on the use of the equipment. My Soldiers used their experience gained from the first half of the deployment to develop and implement new tactics, techniques, and procedures on the use of the equipment and the success rate of the team went through the roof. We were suddenly the most successful and sought after SIGINT platoon in Baghdad. During the second deployment in 2007 to Kirkuk, the Army issued us even more advanced targeting equipment and I still had many of the Soldiers from the first deployment. Additionally, we added some Navy Sailors. These Soldiers and Sailors used innovative thinking and their desire to succeed in their operation of the advanced equipment to cause a significant impact to combat operations by assisting in the capture of over 600 insurgents and persons of interest.

Continued on page 3

Praetorian 6 (cont.)

Continued from page 1

of the devices to be manufactured and installed on U.S. armored vehicles. In the meantime, other units quickly adopted the device and saw the direct operational benefits. Instead of being counseled for unauthorized modifications to U.S. Government property, Sergeant Culin was recognized for his efforts with the Legion of Merit. The award was a small but well-earned token of appreciation for the many Allied lives his innovation saved.

Innovation is a critical component to the Brigade's success, and we must encourage it whenever possible

What can we learn from Sergeant Culin? First, innovative ideas deserve to be heard. We cannot constrain operations based on yesterday's situation. We must constantly and vigorously seek new and innovative solutions to today's problem. Second, leaders must empower their subordinates to innovate. They must do so by understanding the associated risk, mitigating any risk that can't be assumed. Finally, we must recognize and reward innovation. Innovation is a critical component to the Brigade's success, and we must encourage it whenever possible.

1. Innovative ideas deserve to be heard;
2. Leaders must empower subordinates to innovate; and
3. Recognize and reward innovation.

PRAETORIANS

780th MI BDE

"STRENGTH AND HONOR"

Praetorian 7 (cont.)

Continued from page 2

Now I find myself in an organization with some of the most innovative thinkers in the Army. This organization's continued success depends on this "outside of the box" thinking. What you do every day requires creative and innovative thinking. You continue to amaze me on how well you do this. Your ability to think through any problem without a thought of giving up shows your dedication to accomplish the mission. I am proud to be a part of this organization and proud to be your CSM. Continue to think "outside the box" and do the great things you do for this nation.

Praetorians – Strength & Honor

"Everywhere and Always…In the Fight!"

FORT IRWIN, Calif. – *Sgt. Alexander Lecea, Pfc. Kleeman Avery, and Spc. Ashley Lethrud-Adams (right to left), cyberspace operations specialists with an Expeditionary Cyber Team, 782nd Military Intelligence (MI) Battalion (Cyber), brief Col. Brian Vile, commander of the 780th MI Brigade (Cyber), and Command Sgt. Maj. James Krog, the brigade's senior enlisted leader, on their operations as part of the cyber and electromagnetic activities (CEMA) Support to Corps and Below program while supporting training for the 3rd Brigade Combat Team, 1st Cavalry Division at the National Training Center here on January 14. (U.S. Army Photo)*

Vanguard 6: Assignment Incentive Pay

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

Racing for the Soldier.

Once a Vanguard Soldier becomes fully trained and qualified (FT/FQ), a sprint race kicks off to start that Soldier's Assignment Incentive Pay (AIP) as soon as possible. It is my objective to make AIP processing simple, reliable, fast, and transparent—we won't stop innovating until we've met these goals.

Just click "add to cart."

From the Soldier's perspective, I expect AIP processing to be as standardized and as straightforward as submitting for leave. However, in order for us to get to this point, my staff and I needed to fully appreciate how AIP works. The 780th Military Intelligence (MI) Brigade is a part of the Army Cyber Mission Force AIP program, a unique U.S. Army Cyber Command (ARCYBER) program with a unique process. Across the Department of Defense, AIP is used as a general method to compensate military members for successful performance in certain critically—important billets—for the Army this includes Korea assignments, Special Operations Forces, and Cyber. Since AIP is a general tool, DOD regulations place limitations on which level of command can start the pay, how AIP must be tracked and processed, and the standardized formats to be used. In other words, certain parts of AIP processing seem arcane and drawn out to me, but that's because they have to be by regulation. Ultimately, this means that 781st MI Battalion AIP processing is more challenging than the model I most often compare us to—jump pay at an airborne unit. It is my job to oversee an optimized process that gets Soldiers paid within these regulatory requirements.

Getting after it.

The battalion and brigade are innovating to optimize special pay processing. We recently studied the process from end-to-end. We traced where AIP packets traveled and how long each takes along the way. We met with DMPO Meade (Defense Military Pay Office) and ARCYBER to identify pain points across processing, timing, and policy. If you have not seen the results of this analysis, ask your company command teams. Improvements include auditing and metrics, key leader engagements with DFAS, the use of automation across staff sections, and the commitment of battalion resources at bottlenecks. Company command teams are especially innovative in taking care of their Soldiers. I would like to specifically praise the collaborative work that Capt. Hart, Capt. Milchak, Capt. Lanahan and their first sergeants have recently done in conjunction with our S1, Capt. Barajas.

Where we need help.

As a Soldier, you can help ensure your AIP gets started quickly. The most important first step is to anticipate when you will become FT/FQ. Is your last pipeline class coming up? Did you just finish your Job Qualification Record or basic exam? Work with your supervisor, team lead, training room, and company command team to build your packet from the standard battalion template so that it is ready to sign and submit on your FT/FQ date. Second, be aware of the process and periodically on check your packet as it is processed in GEARS. Generally, AIP packets must be signed by your company commander, myself, Col. Brian Vile, and by Mr. Pontius, the Deputy to the U.S. Army Cyber Command commanding general. Along the way, staffs are responsible for checking eligibility and verifying training records. If your packet stalls out somewhere, I want to know about it. Don't get me wrong—each step is responsible for reliably processing and forwarding on your packet—it's just that, you, the packet owner, remain my last safety net.

Continued on page 46

A Nibble on Innovation

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

As I began to think more about innovation, I felt like it's such a broad term that I needed to scope it somewhat to get a better grasp of what it means. The best description that I could come up with is that innovation is the discovery and implementation of new solutions to technical, process, and/or personnel challenges. These solutions can be entirely original, a repurposing of existing solutions, or a hybrid that achieves the desired end state; improved performance and enhanced outcomes. Innovation breathes relevance and vitality into an organization. That said, innovation is not for the faint of heart. It is an arduous endeavor that requires persistence, a solid foundation of knowledge/skill, a sense of curiosity, and initiative to continuously search for and implement new solutions.

Throughout our history, the U.S. has led or been in the forefront of innovative discovery and implementation. This is readily observable through our space program, advancements in technology, and the continued development of our military's weapons, tactics, and training methodologies. Although we have dominated across these areas in the past, we cannot afford to rest as innovation is a competitive space where we can easily be overcome due to a sense of comfort and perceived lasting advantage.

One means to measure America's innovation on a global scale is by referring to the Global Innovation Index (GII). This is a worldwide analysis of innovation across a number of specialties. It may surprise you to find that, while the U.S. has consistently placed in the top ten, it has been ranked no higher than third since 2015. Although this is a bit concerning, it shouldn't be taken as a doomsday alarm. Rather, it serves as a solid reminder that innovation is not limited to U.S. ingenuity, but is a worldwide pursuit across multiple disciplines to see who can attain and maintain the advantage over their competitors.

For more information on the GII, refer to: https://www.globalinnovationindex.org/about-gii

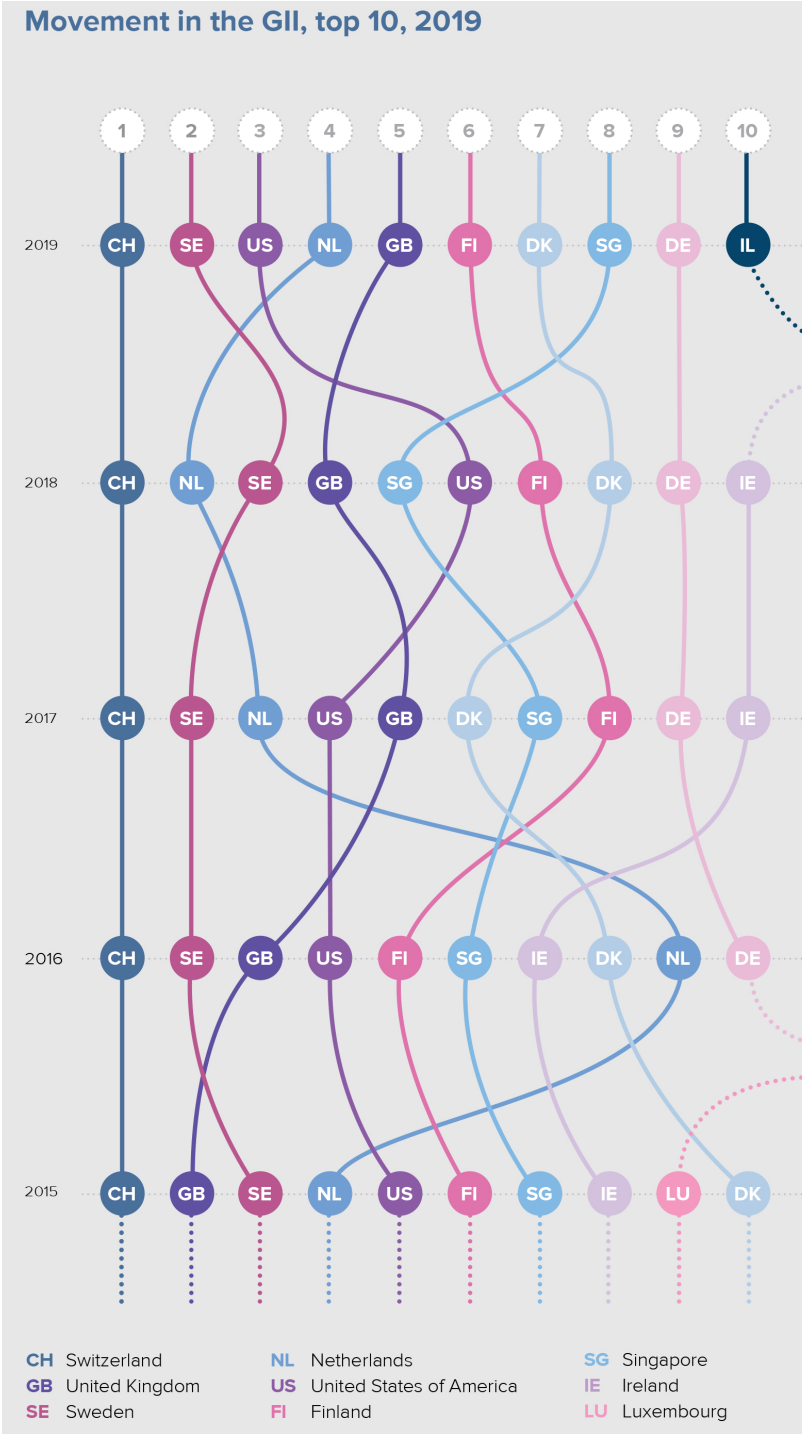


Figure 1: Global Innovation Index 2015-2019

After much self-reflection, I came to the conclusion that innovation may not be my strongest trait. I'm not sure if this is unique to myself, or if this is a common feeling amongst my teammates. As a recognized deficiency, I decided to do a bit of analysis to see if I could come up with some ideas to improve in this area. As I proceeded, I came up with the following thoughts:

People who succeed at innovation are generally:

1. Well educated, trained, and/or experienced in a particular discipline;
2. Think in problems first, then solutions;
3. Take initiative to act;
4. Focus their time and energy on attaining and implementing a solution;
5. Persistent in their pursuit of discovering a solution; and
6. Recognize a solution and act to implement.

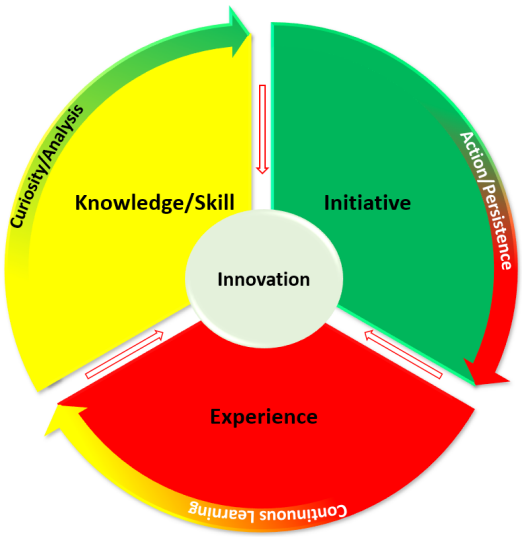


Figure 2: Traits that empower innovation

The Cyber Mission Force (CMF) is a young organization that is growing in structure, education, training, and experience. As the force continues to mature, innovation should be part of the fabric that makes up day to day operations. To make this so, innovation must be embraced at the individual, leadership, and corporate levels. Otherwise, ideas and solutions may never see implementation; the intent of innovation. Within this highly technical mission, continuous learning is readily recognized as a core tenant of success. If formal, informal, and experiential learning lag; performance and outcomes will degrade over time, negatively affecting the success of the mission. To help keep this from happening, I suggest that personnel invest time and energy into leveraging the multitude of available resources that empower the individual to develop their understanding and skill within technical, leadership, and process subject matter. Innovation requires personnel to be well-prepared, which is, in part, a personal responsibility. The following are a few online resources that are readily available to help you get started:

- https://www.safaribooksonline.com/home/ (access to technical writing and videos)

- https://portal.cyberforce.site/home (access to virtual training)

- https://usarmy.skillport.com/skillportfe/custom/login/usarmy/login.action (access to the library)

- https://army.overdrive.com/collection/101577 (requires an MWR library account and PIN)

Continued on page 45

Israel enters the top 10 for the first time in 2019.

In 2018, Singapore makes it to the top 5 of the GII.

The Netherlands entered the top 3 in 2017. Sweden maintained 2nd place for the second time.

Germany re-entered the top 10 in 2016.

Since 2011, Switzerland has ranked 1st in the GII every year.

DK Denmark
DE Germany
IL Israel

Caring, Committed, Coachable – building a culture

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

FORT GORDON, Ga. – *Command Sgt. Maj. Christian Adkison, the senior enlisted leader for the 782nd Military Intelligence Battalion (Cyber), prepares to call the battalion formation to attention prior to a change of command ceremony at the Cyber Fitness Center on June 7. (U.S. Army Photos)*

FORT GORDON, Ga. – Lt. Col. Matthew Lennox, the outgoing commander of the 782nd Military Intelligence (MI) Battalion (Cyber), relinquished his battalion command to Lt. Col. Wayne Sanders, in a change of command ceremony hosted by Col. Brian Vile, the commander of the 780th MI Brigade (Cyber) at Gym 5, the Cyber Fitness Center, on June 7.

Lennox's focus throughout his command has been on collective training, building the core, and enhancing the battalion's Non-Commissioned Officer (NCO) Corps, and what he asked of his Soldiers and Army Civilians was to be "caring, committed, and coachable" in order to build a culture. And that is exactly what they did.

"We built a culture. We have moved beyond in-processing people, pushing them through training, and getting them onto a (cyber) team, to building a Family."

Command is a marathon

Lennox is only the battalion's third commander. He compared his command to a marathon. "The marathon is both the two years that you are in command and the marathon that is just command."

He thanked his predecessor, Col. David Chang for putting things in motion.

"Dave Chang left me a very solid battalion. They had a phenomenal reputation, but what I anticipated was we were never going to be asked to do less. I expected the amount of work, the number of operations, the number of capabilities we needed, to expand," said Lennox. "When I looked across the battalion at the time, we had a lot of individually trained folks and most of the teams – all of the teams were FOC (fully operationally capable) at that point – were on a glide path to come back to a validation exercise. It tended to be a time when teams were trying to do an in-stride assessment or get away from dedicating two weeks a year to actually doing collective training within the team."

Collective Training, the Core, and the Non-Commissioned Officer (NCO) Corps

Lennox, looking back on his two years in command, talked about three focus areas that the Soldiers and Army Civilians seized upon and advanced: collective training, "the core", and the non-commissioned officer corps.

The first was on the value of collective training exercises.

"We have always allocated the time for the teams to do it," said Lennox. "In conjunction with the Joint Force Headquarters, it wasn't always easy, but we got to a place where they enabled the teams to train, and that really set the teams up for success."

Secondly, Lennox said the battalion adopted a term

FORT GORDON, Ga. – *Lt. Col. Wayne Sanders, the commander of the battalion formation at the Cyber Fitness Center on June 7.*

FORT GORDON, Ga. – *Soldiers of the 782nd Military Intelligence (MI) Battalion (Cyber) participated in a battalion change of command ceremony, whereby Lt. Col. Matthew Lennox, the outgoing battalion commander, relinquished command to Lt. Col Wayne Sanders, in an event hosted by Col. Brian Vile, commander of the 780th MI Brigade (Cyber), in front of fellow Soldiers, Family and friends, at the Cyber Fitness Center on June 7.*

for the group of people who "make mission happen" on each cyber team and they called these Soldiers and Army Civilians "the core."

"Early on we decided that each team, on average, had about eight people in 'the core' and the intent was to grow 'the core', over time, to about 20 people," said Lennox. "I think most teams are there today where they've got a core group of 20 people. What that [means] is, if a crisis hits this weekend, you have 20 knowledgeable, practiced people on the team in order to get the mission done."

His third focus area was growing the NCO Corps. Lennox reminisced back to his time when he was a cyber team lead. He said his warrant officers were predominantly the ones leading the sections, training individuals, and taking care of people. He didn't have that NCO backbone like every other unit in the Army.

"One of the things I worked on with Command Sgt. Maj. (Bart) Larango and Command Sgt. Maj. (Christian) Adkison was on growing the NCO Corps.

782nd Military Intelligence (MI) Battalion (Cyber), stands in front of his

Today, Command Sgt. Maj. Adkison is managing a very good NCOPD (NCO professional development) program," said Lennox. "I truly believe we have the NCO Corps that we need to have, both now and in the future, already resident within the battalion. It's a function of having a very good command sergeant major, a function of the best, top of the line first sergeants – six of them were selected for the Sergeant Majors Academy to become sergeant majors – and from there down, the quality of NCOs in this battalion has improved dramatically. It's about taking care of Soldiers."

According to Lennox, those three focus areas enabled his command philosophy.

"What I really wanted when I came into the battalion was for people to be 'caring, committed, and coachable'. Those were the three words I used throughout my time in command. Every time I talk, I talk about those three terms. I believe that if you are those three things, then you are the leader that we need in this organization."

Caring, Committed, Coachable

Lennox explained that caring is taking care of yourself, taking care of your Soldiers, and taking care of your Family; and committed means driving the organization to success, understanding what the mission is, and what is going on two levels up.

"Those are just Army fundamentals, things you are taught from the time you're a lieutenant in Combat Arms," said Lennox. "Coachable is a new domain in that we are all going to make mistakes, and I'll underwrite the honest mistakes in cyber operations

Continued on page 43

Servant Leadership – a true backbone of the

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

FORT GEORGE G. MEADE, Md. – *The official party consisting of (left to right) Command Sgt. Maj. James Krog, the senior enlisted leader for the 780th Military Intelligence (MI) Brigade (Cyber); Sgt. Maj. of the Army Kenneth O. Preston, the keynote speaker; Command Sgt. Maj. Jesse Potter, the senior enlisted leader for the 781st MI Battalion (Cyber); and Sgt. Maj. Jonathan Coleman, Noncommissioned Officer-in-Charge for the Brigade S-3 (operations) section, 780th MI Brigade, listen to narrator as he discusses the importance of the NCO Induction ceremony on June 3 at the Post Theater. (U.S. Army Photo)*

FORT GEORGE G. MEADE, Md. – The 780th Military Intelligence (MI) Brigade (Cyber) hosted a Non-Commissioned Officer (NCO) Induction Ceremony for 26 recently promoted NCOs on June 3 at the Post Theater.

The keynote speaker for the event was Sergeant Major of the Army Kenneth O. Preston, who served as the 13th Sergeant Major of the Army (SMA) from January 15, 2004, to March 1, 2011. He retired as the longest-serving Sergeant Major of the Army, with more than seven years in the position.

"It was an honor having Sergeant Major of the Army Kenneth O. Preston help us with inducting our new NCOs into the Non-Commissioned Officer Corps," said Command Sgt. Major James Krog, the 780th MI Brigade's senior enlisted leader.

Preston primarily focused on two things in his remarks to the newly inducted NCOs. First, he stated that NCOs are trainers, "they are the teachers for that portion of the Army we give them responsibility for," and the second thing he mentioned was that they should lead by example.

Preston also stated the importance of lifelong learning.

"When you look at the demands on the Army today – particularly first-line supervisors – and as Soldiers progress through the Army and take on positions of increased responsibility; learning never stops," said Preston. "The other piece of advice is 'lifelong learning'. It never stops. You always continue to read and do the professional development, because it is what keeps you the subject matter expert for that piece of the Army you are responsible for."

According to Krog, the NCO Induction Ceremony is an important milestone in a Soldiers career as the event signifies their transition from "being one of the followers to also being a leader."

"The Soldiers in this Cyber brigade are some of the smartest in the United States Army. It's important for them to see and experience this transition from enlisted to NCO because it shows a transformation from being one of the followers to also being a leader," said Krog. "The NCOs in this brigade need to understand they must not only be technically proficient, but they must also be leaders. The Soldiers below them need that leadership and expect that leadership."

Krog also believes NCOs are servant leaders.

"Servant leadership is a watchword for how these Soldiers should serve as NCOs in the Army," said Krog. "Every action they take as an NCO

Army – Past, Present, and Future!

should either be taking care of their Soldiers or accomplishing the mission. I firmly believe my sole responsibility is to take care of every Soldier and Army Civilian in this brigade and I strive to do that every day."

The 780th MI Brigade and the United States Army welcome the following Soldiers into the NCO Corps:

- Sgt. Jeffrey Akers, C Compay, 781st MI Battalion
- Sgt. Sheridan Ayala-Eggestein, C Co., 781st MI BN
- Sgt. Sean Brown-Reed, C Co., 781st MI BN
- Sgt. Skyler Bryant, E Co., 782nd MI BN
- Sgt. Daniel Butler, C Co., 781st MI BN
- Sgt. Marcner Charles, A Co., 781st MI BN
- Sgt. Teresa Corbett, C Co., 781st MI BN
- Sgt. Albert Cottam, C Co., 781st MI BN
- Sgt. Justin Devenport, C Co., 781st MI BN
- Sgt. Tyler Gantt, C Co., 781st MI BN
- Sgt. Linda Hanstein, C Co., 781st MI BN
- Sgt. James Harris, A Co., 781st MI BN
- Sgt. Marlee Jackson, A Co., 781st MI BN
- Sgt. Jeffery Jento, C Co., 781st MI BN
- Sgt. David Koski, C Co., 781st MI BN
- Sgt. Brandon Lee, E Co., 782nd MI BN
- Sgt. Devin Lee, D Co., 781st MI BN
- Sgt. Michael Miano, E Co., 782nd MI BN
- Sgt. Andrew Miller, A Co., 781st MI BN
- Sgt. Joshua Peddy, C Co., 781st MI BN
- Sgt. Justin Radanovic, C Co., 781st MI BN
- Staff Sgt. Jackson Rolf, E Co., 782nd MI BN
- Staff Sgt. Jeffrey Schmidgall
- Sgt. Jeffrey Spilker, C Co., 781st MI BN
- Sgt. Derek Tien, A Co., 781st MI BN
- Sgt. Aisha Umar, D Co., 781st MI BN

FORT GEORGE G. MEADE, Md. *– Recently promoted Noncommissioned Officers (NCOs) assigned to the 780th Military Intelligence (MI) Brigade (Cyber) recite the Charge of the Noncommissioned Officer, one of the significant events of the NCO Induction Ceremony hosted by the 780th MI Brigade on June 3 at the Post Theater. (U.S. Army Photos)*

FORT GEORGE G. MEADE, Md. *– Sgt. Sheridan Ayala-Eggestein, C Company, 781st Military Intelligence (MI) Battalion receives his 'Charge of the Newly Promoted Noncommissioned Officer" certificate from Command Sgt. Maj. James Krog, the senior enlisted leader for the 780th MI Brigade (Cyber), while Sgt. Maj. of the Army Kenneth O. Preston, looks on at the Post Theater on June 3.*

Vanguard 7 signs off the net to assume greater

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

FORT GEORGE G. MEADE, Md. – *Lt. Col. Nadine Nally (right), commander of the 781st Military Intelligence (MI) Battalion, presents a farewell gift to Command Sgt. Maj. Jesse Potter, the battalion's departing senior enlisted leader, on behalf of the unit's Soldiers and Army Civilians, before a Relinquishment of Responsibility ceremony at the post theater on July 1. (U.S. Army Photo)*

FORT GEORGE G. MEADE, Md. – Soldiers and Army Civilians of the 780th Military Intelligence (MI) Brigade (Cyber) bid farewell to Command Sgt. Maj. Jesse Potter, the departing senior enlisted leader for the 781st MI Battalion (Cyber), and his Family during a Relinquishment of Responsibility ceremony at the post theater on July 1.

Although he only served as the battalion command sergeant major for 15 months, Potter leaves behind an enduring legacy as he and his Family move to Fort Gordon, Georgia, where he will assume even greater responsibility as the senior enlisted leader for the U.S. Army Cyber Command's Cyber Protection Brigade on August 15.

The 781st MI Battalion is also known as the "Vanguard," their motto "When Others Cannot". Potter is often referred to as Vanguard 7, his military call-sign.

In her remarks, Lt. Col. Nadine Nally, commander of the 781st MI Battalion and the host for the ceremony, talked about Vanguard 7's character, legacy, and his fondness for Spartan obstacle races.

"Mission Command, Empowerment, Communication, Opportunity and Teaming – Command Sergeant Major not only evangelized it, he lived it. Throughout his tenure as Vanguard 7, he has protected this house and defined what it means to embody the Vanguard ethos," said Nally. "At any given moment, he would stop to help the Vanguard Soldiers and Civilians."

Nally said it was Potter who enabled the battalion to present a trained and ready unit for the Cyber National Mission Force.

"His steadfast aim of building a cyber force of the future, while also meeting current mission demands of this battalion with a scope, scale and complexity of operations rarely seen, even at brigade-levels, achieved superior results," said Nally.

In addition to his providing candid feedback to the command team, empowering the non-commissioned officer (NCO) Corps, and advising the officers and Civilians, Nally talked about Potter's significant accomplishments during his tenure: attaining a 95 percent Soldier deployable rate, exceeding U.S. Army Intelligence & Security Command and Army requirements; building a Spartan Agoge-based leader development program; partnering with the 10th Mountain Division NCO Academy and Light Fighter School, resulting in 18 brigade Soldiers graduating from the Air Assault course and four Soldiers becoming rappel masters; 90 specialists graduating from the Basic Leader Course; and two Ranger course graduates.

Potter, in his remarks, described his most memorable moment as building a 'teaming' culture.

"When I came to the battalion, we had just completed the build and declared all of our teams FOC (fully operational capability). The culture of the organization was split between the Cyber Soldiers and Military Intelligence Soldiers," said Potter. "Over the last

Continued on the next page

cyber responsibilities

Continued from the previous page

15 months of truly embracing and enabling one of Lt. Col. Nally's leadership tenants of 'teaming,' we now have a culture that embraces the team of teams approach. This has paid huge dividends operationally across the entire formation."

Vanguard 7's departing advice for the Soldiers and Civilians will resonate with all those who have served with him.

"I would be remiss if I didn't remind (the Soldiers and Civilians) to get their grill fixed, get off the computer, and go outside and do some type of physical challenge," said Potter. "To continue to seek balance both in your life and career, seek constant improvement, and 'be the Lion, not the sheep; be the leader, not an insignificant member of the herd.'"

Potter ended his remarks with these parting words: "Look at the Soldier to your right and left; you will draw strength from them, as they will draw strength from you. You will not let them fail! Because we are the VANGUARD!"

"Vanguard 7, 'Yando,' signing off the net."

Vanguard conquers the Spartan Stadion

WASHINGTON, D.C. – *Lt. Col. Nadine Nally, the battalion commander for the 781st Military Intelligence Battalion (Cyber), Command Sgt. Maj. Jesse Potter, the battalion's senior enlisted leader, along with the company command teams, primary staff officers and noncommissioned officers, and their Family members, conquered the Spartan Stadion Honor Series Race at Nationals Park May 11, and all displayed a true warrior spirit. (U.S. Army Photos)*

INSCOM's Best Warrior NCO and Soldier of the Year

By Jocelyn Broussard, deputy public affairs officer, U.S. Army Intelligence and Security Command

FORT A.P. Hill, Va. *-- Spc. Eva Perry (right) from Issaquah, Washington, is the 2019 Soldier of the Year and the 780th Military Intelligence Brigade (Cyber) Best Warrior (Soldier), and Sgt. Kyle Tamraz from Saylorsburg, Pennsylvania, is the 2019 Noncommissioned Officer of the Year and brigade's Best Warrior (NCO). Both of these Brigade Soldiers participated in the U.S. Army Intelligence and Security Command (INSCOM) Best Warrior Competition from June 1 - 5. (U.S. Army Photos)*

FORT A.P. HILL, Va. -- The U.S. Army Intelligence and Security Command (INSCOM) hosted its 2019 Best Warrior Competition (BWC) during the week of June 1-5.

Soldiers competing represented the best of the best from three geographic regional competitions, and two categories (Noncommissioned officers and Soldiers). Their single goal, conquering the four-day mental and physical challenges, leading one Soldier and one noncommissioned officer (NCO) to victory.

On June 6, the INSCOM winners were announced by Sgt. 1st Class Peter Heap, the BWC event noncommissioned officer in charge (NCOIC) during an award ceremony held at INSCOM headquarters, Fort Belvoir, Virginia.

Sgt. Kyle Tamraz, a signal intelligence analyst from the 780th Military Intelligence (MI) Brigade, was titled the INSCOM Best Warrior NCO of the Year.

Spc. Jacob Olive, a wheeled vehicle mechanic from the 66th MI Brigade was titled the INSCOM Best Warrior Soldier of the Year.

Each winner was presented with the Army Commendation Medal by Maj. Gen. Gary Johnston, INSCOM's commanding general, followed by Command Sgt. Maj. Eric Schmitz, INSCOM's command sergeant major, presenting the winners with a bronze trophy.

Tamraz, a Saylorsburg, Pennsylvania native, assigned to the 781st MI Battalion (Cyber), 780th MI Brigade, Fort Meade, Maryland, made the competition his number one priority, putting his best foot forward and giving it his all to become the 2019 Best Warrior NCO of the Year.

"Winning the competition is a huge accomplishment for me," said Tamraz "I think the best warrior competition makes you a better soldier because of the dedication and time that has to go into competing. While not only performing your everyday job, you are also constantly studying and preparing for the next level. This also allows you to become a knowledgeable leader that soldiers can go to for advice and questions. I will be focusing on preparing for the board and more warrior tasks and battle drills. I look forward to the next level competition."

The competition made each of the competitors dig deep to push themselves beyond the limits.

INSCOM Best Warrior Solider of the Year, Olive, a Hayfield, Minnesota native, assigned to the Headquarters and Headquarters Company, 66th MI Brigade, Wiesbaden, Germany, gave credit to his sponsor, and his maintenance team for preparing and

FORT A.P. Hill, Va. *-- Sgt. Kyle Tamraz, B Company, 781st MI Bn., participates in a Leaders Reaction Course event on day three of the U.S. Army Intelligence and Security Command Best Warrior Competition on June 5.*

motivating him to compete.

"My sponsor and my maintenance team motivated me to compete in this year's competition," said Olive. "Throughout the preparation for this competition, I learn my physical limits and how hard I can push myself."

"I'm happy and proud to have won. I'm thankful to my maintenance team, sergeants and sponsor for helping me to get this far. This competitions showed me my strengths, weaknesses and what I need to continue to work on."

The four-day competition challenged the Soldiers with a variety of tasks to include the Army Physical Fitness Test, an obstacle course, day and night land navigation, weapons systems qualification, situational warfare training exercises, a 12-mile ruck march, the leader's reaction course, a formal board, a written exam and more.

According to Heap, who assisted with the facilitation of the BWC events, this year.

"12 out of the 13 events went as planned," said Heap. "Each of the competitors were determined, competent, and flexible in the face of adversity and came prepared for each event."

"I was impressed by the comradeship the competitors showed to each other," Heap added. "Many of these NCOs and soldiers know each other from previous duty stations and that relationship is evident when they show up to the best warrior competition. Their intent is to beat each other, yet it was quite impressive on events such as the LRC [leaders' reaction course] or 12 mile road march to see the soldiers encouraging each other. This year was different with the amount of fellowship between them."

Tamraz and Olive will move on to the next level, the U.S. Army Cyber Command Best Warrior Competition, scheduled to take place, July 22-26 at Camp Upshur, Quantico, Virginia.

Both winners expressed gratitude to their leadership, family and friends for supporting them leading up to and throughout the Best Warrior Competition.

Although the Best Warrior Competition is an annual event, the evaluated events are designed to not only test the competitors' skills, strengths and knowledge but it also prepares them for the operating environment as it continues to evolve each year. Readiness is the U.S. Army top priority therefore competitions like these are always a great way to challenge individuals to put their skills into action outside of their unit training.

Congratulations to all the INSCOM BWC competitors for your hard work and commitment.

Noncommissioned Officer (NCO) category:

- Sgt. Kyle Tamraz, 780th MI Brigade
- Sgt. Ethan Meador, 66th MI Brigade

Soldier category:

- Spc. Jacob P. Olive, 66th MI Brigade
- Spc. Jonathan Carter, 116th MI Brigade
- Spc. Eva Perry, 780th MI Brigade

FORT A.P. Hill, Va. *-- Spc. Eva Perry participates in a stress shoot on day two of the U.S. Army Intelligence and Security Command Best Warrior Competition on June 4.*

Securing the Network Footprint:

Modernization of PON in the Army Cyber community

By Capt. Tore Girty, BN S6, 781st Military Intelligence Battalion (Cyber)

Consolidation of IT assets to fulfil DOD's energy and power conservation efforts, while improving the cybersecurity posture has been an Army mandate since 2011. In recent years, the Army's Military Intelligence and Cyber communities have begun to integrate Passive Optical Network (PON) technology in order to achieve both requirements simultaneously. The PON technology has been most commonly utilized by Internet Service Providers (ISPs) to bring fiber to the home, but the same benefits it provides to them can be applied into a military environment as well. The traditional network infrastructure takes a three-layer approach: core, distribution, and access. This type of network infrastructure creates a need for multiple intermediary devices at each layer to achieve redundancy and reduce the impact of outages, but in doing so it also increases the amount of avenues of attack an adversary can utilize to compromise a network.

The PON technology collapses the distribution and access layers into a single, flat infrastructure through a point-to-multipoint fiber distribution, utilizing upstream and downstream signals over a single fiber cable. By implementing PON technology, a large three floor facility requiring twenty communication closets and over fifty intermediary devices can be reduced to three closets and six PON devices to achieve the same results. The PON system replaces each common access layer switch with an unpowered, unmanaged fiber splitter and an Optical Network Terminal (ONT) for end user network access. It also carries a significant reduction in cabling requirements due to each intermediary device, only requiring a single backbone fiber cable for several hundred end users. This innovation considerably reduces infrastructure compared with a traditional point-to-point architecture.

With less IT infrastructure, the Army will maintain less devices for an adversary to target and allow its administrators to focus on hardening and monitoring fewer devices. However, as with any newly adopted technology, the Army has a process to certify and accredit a technology that must be completed prior to operational capability. The Army employs the National Institute of Standards and Technology's (NIST) Risk Management Framework (RMF) to facilitate the proper and secure integration of technologies into the DOD Information Network (DODIN) through a seven-step risk management process. The 781st Military Intelligence Battalion has recently become the first Army unit to successfully submit their body of evidence for an RMF site assessment of a PON system on a highly classified network. While many units currently utilize PON on various unclassified and commercial networks, it is exceptionally challenging when elevating technology to a higher classification. The S6 staff of the 781st have worked alongside cybersecurity professionals from DIA, NSA, and INSCOM over the span of eight months to accomplish this goal. Their efforts will pave the way for many organizations within DoD, as well as intelligence and cyber communities to adopt the benefits of PON into their IT infrastructure.

A solid cybersecurity posture requires an organization to give the freedoms of initiative and innovation to their IT and cyber professionals. Often times, where the government is concerned, these actions are over shadowed with other competing requirements. However, on occasion an organization decides to accept the challenge and navigate obstacles in order to introduce a new, innovative solution. In this case, the 781st has picked up the torch and begun lighting the way for an Army-wide PON integration through global information-sharing and collaboration with multiple Network Enterprise Centers (NECs), Ground Support Intelligence Activities (GISAs), and Signal commands.

Innovative Training: Attack and Defend

By 2nd Lt. Sean Little, B Company, 781st Military Intelligence Battalion (Cyber)

Credible Army training is tough. Limited resources and a surplus of distractions plague all the branches of the Army. In the Cyber branch, the scope of this problem is multiplied because we are still a nascent branch; all of our training resources have not yet been developed or identified. When Capt. Alexander Master of Bravo Company (Co.), 781st Military Intelligence (MI) Battalion encountered this issue within his own organization, he decided to create those training resources himself.

Working with Brigade S6 (signal/IT), he identified several servers and laptops that were available and determined they could be used to create a virtual training environment. With this hardware in mind, Capt. Master came up with the idea to create a cyber-range for B Co. to use in its own 'Attack and Defend' exercise.

Once Capt. Master established the parameters and his intent, he designated two talented Cyber Soldiers as the officer-in-charge (OIC) and noncommissioned OIC and instructed them to bring the plan to fruition.

These Soldiers developed a scenario in which a blue team defended 15 virtual machines running a plethora of vulnerable software applications, and a red team attempted to exploit and gain access to the vulnerable apps. The Soldiers in charge utilized a combination of Discord, GitHub, and GitKraken to organize their progress, dedicating much of their time outside of the workday to complete the exercise on time. The OIC and NCOIC developed rules of engagement, set up the software on the different virtual machines, and came up with a realistic background story to tie the whole exercise together.

In the fictional scenario, the red team worked for a private security firm that was hired to take down the *Vanguard Technology Conglomerate*, a fictional mega-corporation whose rapid and ruthless acquisition of the technology and information industries has threatened to put hundreds of smaller corporations out of business. The red team's primary goals were to acquire and maintain access to network nodes inside of target space, ex-filtrate or destroy sensitive data, and remain undetected by the adversary. On the other side, the blue team had been hired by the *Vanguard Technology Conglomerate* to perform incident response on the network after suspicious traffic was detected. The blue team's primary goals were to contain the spread of the red team's access to the network, eradicate the red team's presence on enterprise network, and maintain Internet connectivity to the network.

The exercise kicked off at 8 a.m. on June 26 at McGill Training Center with the red team beginning their attack and the blue team arriving an hour later to perform their incident response. The facilitators split the majority of their time roaming the room, assisting the participants during the exercise, and maintaining the server and training environment as the participants navigated through the network. The first day of the exercise resulted in a resounding win for the blue team as they locked out the opposing team with a simple firewall rule. This prompted the facilitators to establish a set of rules of engagement that each time had to abide by.

The next few days of the exercise resulted in the facilitators making changes on-the-fly, including adding a chat room to facilitate discussion between teams, as well as adding company personas (IT tech support, disgruntled employees, etcetera) to the chat rooms. Adding these characters allowed for a new dimension of interaction between the exercise participants and the "characters". At one point, a red-team member convinced a disgruntled employee to create a new user account for the red-team to use to log into a machine on the blue-team network. Logging into a box in a few seconds is much faster than trying to hack into a box.

In an innovative twist, Bravo Company decided not to limit the training to only 17 series (cyberspace operations) Soldiers and instead integrated its

Continued on page 44

Insights from the 2014-2018 Russian Active Measures Campaign

By Capt. Frederick R. Ulrich, B Company, 782nd Military Intelligence Battalion (Cyber)

In February, 2016 the Grand Jury for the District of Columbia indicted thirteen individuals (of Russian Nationality) and a business entity for knowingly and intentionally conspiring to "defraud the United States by impairing, obstructing, and defeating the lawful functions of the government through fraud and deceit for the purpose of interfering with the U.S. political and electoral processes, including the presidential election of 2016" from 2014 to present day [1]. The publicly available indictment and the Report on the Investigation into Russian Interference in the 2016 Presidential Election [2] detail a synchronized set of Information Operations (IO) on various social media platforms with the purpose of interfering in the 2016 Presidential Elections.

During the 2016 presidential election and the years leading up to it, the Internet Research Agency (IRA) sent employees to the U.S. to investigate the political/social climate, integrated their findings into mass social media campaigns, and performed targeted advertisements in order to influence certain demographics of people. Ultimately, the IRA's Information Operations sowed discord in the American electoral process and helped polarize public political discussion.

What made IRA's approach so unique that it could not be predicted and stopped?

Fork online personas into main and auxiliary accounts

The IRA partitioned online personas into main accounts, which posted information, and low equity auxiliary accounts (botnet) that amplified a particular post through links and reposts. For each type of account, the IRA either employed representational populations or notable accounts that are more akin to thematic groups organized by political action entities or geographical location. For example, the IRA employed religious accounts with names "United Muslims of America" and "Army of Jesus" and geographical-oriented accounts like "South United" and "Heart of Texas" [1]. These group accounts appeared to have two purposes 1) retweet IRA content in order to build follower counts and amplify messages and 2) recruit U.S. persons to hold rallies related to the group's message.

IO is a Dish Best Served Warm

The IRA directed its content creators, called "specialists," to "create political intensity through supporting radical groups, users dissatisfied with [the] social and economic situation and oppositional social movements" [1]. The IRA created accounts on both sides of contentious issues such as immigration and race relations [1]. In all cases, opposing political groups controlled by the IRA would agree on the fundamental tenants of the IRA message: the electoral process was rigged and one of the candidates was particularly corrupt [1, 2]. In this maelstrom, the IRA sought to deliver their IO effect, sow discord in the American political process.

Quantitative Measures of Performance and Measures of Effectiveness

The organizations used metrics such as "ratios of text, graphics, and video to use in posts; the number of accounts to operate; and the role of each account" in order to provide concrete ways for specialists to improve their content, presence, and authenticity [1]. The Report on Russian Interference [2] states that the IRA purchased "over 3,500 advertisements" on Facebook which amounted to around $100,000. The Facebook ad platform and other related tools for social media engagement can provide further tools for MOP/MOE which the IRA surely used.

In aggregate, these approaches demonstrate how IO is more useful than ever provided that one uses the modern tools available.

References

[1] *Internet Research Agency Indictment.* https://www.justice.gov/file/1035477/download

[2] *Report on the Investigation into Russian Interference in the 2016 Presidential Election.* https://www.justice.gov/storage/report_volume1.pdf

Fostering technological innovation in our organization

By 2nd Lt. Austin Heath, 200 Combat Mission Team, 782nd Military Intelligence Battalion (Cyber)

"In the innovation centers of America, employees view their organizations in Venn diagrams […], the overlap in the diagram is a source of strength and an engine of innovative thinking. Military organizations too often operate within silos, working independently on projects with rigid adherence to process and bureaucratic norms." — Col. Jason M. Brown, USAF, *Why the Military Needs a Technology Revolution [1].*

Innovation encompasses creativity and autonomy, for it's meritocratic by nature driven by those with motivation and expertise. The Cyber Mission Force cannot afford to neglect fostering a culture of innovation as technology—and our adversaries' use of it—changes daily. Innovation is known for its disruptive nature, so how can leaders of a fledgling branch seek to inspire innovation within its ranks while being beholden to an organization known for its rigidity and adherence to structure?

Leaders within the Cyber Branch should fundamentally be curious and dedicated to continuing their technical education. This profession is inherently unique, if one becomes complacent, they will quickly find their skills and knowledge obsolete. This means more than just following academia, as academic institutions and formal learning also struggle to keep up with the speed at which technology advances. Professionals in this field must take that extra step to become involved within the tech community—treat it more like a hobby rather than a day-job—and have a passion to tinker and discover new ways to solve today's problems. Innovation within an organization starts from the bottom-up, yet, leaders must arm themselves with the requisite knowledge to nurture an innovative culture.

Curiosity is the driving force behind innovation and leaders must value those individuals within the organization who challenge the status-quo. Leaders should look to guide that raw creativity and determination, providing driven individuals a path to explore their ideas and a method to express their innovative abilities. Conversely, innovation requires time, resources, and an acceptance of risk. There is no guarantee that a new project will succeed and with a project's failure, leaders should not look to place blame but rather seek to learn from that failure. Failure is an intrinsic part of innovation, and leaders must ensure that they foster an environment in which it is acceptable to fail, learn lessons from that failure, and make changes for a better future.

Leaders must foster a dialogue within the organization. Sharing is a key factor of innovation as it prevents an organization from having to relearn everything as teammates come and go. It does not do an organization any good if each team internalizes their lessons learned, neglecting to share vital information with those around them. Sharing also facilitates the melding of many minds, allowing innovators to bounce ideas off of one another and forcing best ideas to percolate to the top. Leaders should look to build connections between innovators within the organization, creating relationships that allow people to receive additional support or connections to leverage that they—otherwise—might not have.

In summation, soldiers with diverse technical abilities, drive, and natural curiosity pioneer the future of the Cyber Branch. We as leaders must promote an environment based upon continuous learning, autonomy, and collaboration to stimulate the innovative aspects of our Soldiers, ensuring our branch continues to be the most dynamic, inventive, and adaptive organization in the Army.

Works Cited

1. Brown, Jason M. "Why the Military Needs a Technology Revolution." *The National Interest*, The Center for the National Interest, 1 June 2017, nationalinterest.org/feature/why-the-military-needs-technology-revolution-20933.

OPERATION KU: Combining MOS-specific skills

By 1st Lt. Raymond Goldberg, Detachment-Hawaii, 782nd Military Intelligence Brigade (Cyber)

***SCHOFIELD BARRACKS, Hawaii** -- Soldiers of Detachment Hawaii (DET HI), 782nd Military Intelligence Battalion (Cyber), planned and executed an innovative training exercise named Operation Ku. The operation was built to combine Warrior Tasks and Battle Drills and MOS-specific skills into a single fluid exercise in order to test Soldiers and increase unit cohesion. (U.S. Army Photo)*

SCHOFIELD BARRACKS, Hawaii -- Innovation comes in many forms. While most people view innovation in terms of technological and scientific advancement, that is not always the case.

New challenges constantly arise, which demands Soldiers, Sailors, Coast Guardsmen, and Airmen to come up with new ideas to overcome these obstacles. For the Soldiers of Detachment Hawaii (DET HI), 782nd Military Intelligence Battalion (Cyber), the challenge for innovative thinking came from a training necessity.

DET HI planned and executed an innovative training exercise named Operation Ku. The operation was built to combine Warrior Tasks and Battle Drills (WTBD) and MOS- (Military Occupational Specialty) specific skills into a single fluid exercise in order to test Soldiers and increase unit cohesion.

The DET HI command team, like the rest of the Army, understood there is an annual requirement to test every Soldier on their Warrior Tasks and Battle Drills (WTBDs). The obvious course of action is to throw together an exercise which 'checks the box', and have all the Soldiers slog through it in order to fulfill the required training.

However, Lt. Col. Jason Hogan, the DET HI commander, believed executing WTBD in this fashion would decrease morale within the unit (not everyone joins Cyber because of the 1337 field work). Instead, a new plan was hatched; one that required a mix of WTBDs and MOS skill level 1 tasks.

"OPERATION KU was designed to reinforce WTBDs in a field environment in combination with the addition of what is normally garrison, MOS skill level 1 tasks," said Hogan. "The STX (situational Training Exercise) lanes were designed to stress team leadership, basic level understanding of WTBD, and demonstrate that Military Intelligence and Cyber Skill level 1 tasks have tactical, "real Army" applications. My vision was to provide the Soldiers and Civilians of the Detachment an environment outside the norm that helped bond the unit over some shared misery of the field environment. Cyber must build and implement innovative training situations to really challenge and build a team of teams. By combining WTBD and MOS technical tasks in a field environment, we can truly assess the whole Soldier or Civilian."

Ku (pronounced "coo", with a hard "c") is the name for one of the primary ancient Hawaiian gods. While Ku is widely known for being the god of war, he also has overlapping responsibilities with other gods, such as being the god of farming, forest and rain, and fishing.

with Warrior Tasks and Battle Drills

What makes Ku an apt name for the DET HI exercise is that Ku is also a god of sorcery, which many believe is reminiscent of today's Cyber actors. To others outside our career field, hackers are seemly able to accomplish feats of near-magical quality with little effort on their part. We know better, of course, but this mixture of war and sorcery are what formed a basis for our operation. This article describes how Operation Ku was executed, and how the Soldiers of DET HI rose to the challenge of combining two seemingly disparate skills to accomplish the mission.

For the Soldiers, the day started at 6 a.m. with a formation at the East Range parking lot. It was a cloudy morning, with scattered light rain and temperatures in the low to mid 70s. Despite the early hour, the sun was already coming up, which negated the use of red lenses from the beginning of the event. Once accountability of Soldiers and equipment was completed, the competitors were split up into teams, dependent on what part of the unit they were in: Analysis and Production (A&P), Operations and Plans, and the Cyber Support Team (CST).

At 6:30 a.m. the Soldiers started the operation with a 1-mile ruck march to the Assembly Area (AA) on a dirt road. The teams handled the march well, and made good time to the AA, which was a small clearing inside the woodline next to a landing area. East Range was very quiet that day; only the occasional government vehicle passed us by on the way in. While the range doesn't support live-fire exercises, it is home of the Army's Jungle School and hosts the 25th Infantry Division's NCO academy during field days, which makes it a relatively active range for most of the year.

Once all teams were in position at the AA, Lane Graders would begin briefing each of the teams' Platoon Leadership their Operation Orders (OPORDs). Operation Ku was split up into three Situational Training Exercise (STX) Lanes, each of whom was focusing on different skills that the Soldiers were briefed on. The movement scheme of the whole operation was based on a "hub and spoke" method; a team would go out to an objective, return to the AA, receive another OPORD, and repeat the process three times. Since I was the Unit Public Affairs Representative, I decided I would go out on each of the lanes, but with a different team every time, that way I was able to get photos of each lane and each team.

Lane 1's main objective was to secure an intelligence cache and report back to higher HQ about what it is. While there were no Opposing Force (OPFOR) personnel on this lane, none of the teams knew that, and had to act as if they were going to receive contact at any time once the lane was under way. I went on Lane 1 with the A&P team, under the leadership of 1st Lt. Maroni and Staff Sgt. Watson, during the last rotation of the day. As luck would have it, the rain started coming in heavier once A&P reached their objective, which forced Maroni and the two Language Analysts (LAs) (Staff Sgt. Mrugalski and Sgt. Neal) to huddle underneath the small poncho lean-to that marked the intel cache. The LAs seemed to have a good time throughout the exercise, since

Continued on the next page

Staff Sgt. Mrugalski (left) translates information found on an objective in Lane 1, while 1st Lt. Maroni (right) observes and communicates with higher headquarters. (U.S. Army Photo)

OPERATON KU

Continued from previous page

this gave them a chance to test their skills "on the fly" in an operation. On their way back to the AA, I heard the banter between the two LAs and a Lane NCO Sgt. Smith (also and LA) about the finer points of the translation they conducted, expressing interest into why certain words and terms were used. The lane went very well, although it should be noted that Sgt. Neal, ever the pessimist (or a realist, as he routinely corrects us of), seemed strongly dissatisfied with the rain.

Lane 2 and 3 consisted of searching enemy personnel and finding a weapons cache, respectively. The CST was running through Lane 2 when I walked with them, and Operations/Plans oversaw finding the weapons cache at Lane 3. Both lanes went very well, with the teams and OPFOR playing their roles flawlessly. On the subject of OPFOR, Staff Sgt. Pate and Spc. Deutsch played the role of peaceful villagers/ OPFOR in Lane 2, whom needed to be searched, but the role-players did not know English and seemed aloof to a lot of the CST's attempts at communication, which gave Pfc. Camp and Cockerham (the Soldiers conducting the search) no end of frustration. On Lane 3, Staff Sergeants Rah and Horne conducted a near ambush of Ops and Plans Team. Horne ended up dying tragically in a way reminiscent of the movie Platoon, but Rah seemed immune to notional bullets; nimbly dodging all of them and managing to escape.

Once all the teams managed to get through each of the lanes, they moved on to the culminating exercise where they had to find a way into the network of a military bunker and complete a specific objective. Each team was responsible for one of the following: shutting off primary power, auxiliary power, or opening the main door. All of this was supposed to be in support of the 25th ID assaulting the aforementioned bunker, which was symbolized by a miniature model made out of cardboard and paint, complete with green army men. On top of that, they had to use "intel clues" that the teams found during the initial lanes IOT move forward in the challenge.

"I liked how each mission gave us a clue that would be needed in the culminating challenge," said Staff Sgt. Watson. "I know a few Soldiers were blown away by the detail that was put into the culminating challenge, especially the interactive model built by Chief Warrant Officer 2 Howard. I could tell there was a lot of thought and work put into Operation Ku. I thought it was a lot of fun, and it brought our team together."

The competition was fierce, with all teams completing their assigned task within close time proximity to each other, however Ops/plans was able to finish first.

In closing, Operation Ku was a success because of the Soldiers' positive attitude throughout the day, as well as an excellent staff that worked hard make the operation go off without a hitch. At the end of the day, three cadre were given Detachment coins for their valuable contributions: Staff Sgt. Crooke, CW2 Howard, and Sgt. 1st Class Gallaway. 1st Lt. Ballou was crowned MVP of the operation, because of the outstanding leadership he demonstrated through each of the lanes. Finally, Ops/plans came in first place for Operation Ku and got to take home the highly coveted "Ku Trophy", to be displayed at work until the next competition.

Flexible, adaptive and fully situationally aware cyber leaders

By Staff Sgt. John Pederson, Unit Public Affairs Representative, Detachment Texas, 782d MI Battalion (Cyber)

Training and retaining leaders in the military cyber operation field presents unique challenges. The cyber branch does a fantastic job in developing necessary technical skills. The amount of training personnel receive while pursuing a career in the military cyberpace operational realm is staggering. There has been a great deal of innovation on how we train, such as partnering with and colleges to train specific skills and developing relationships with industry-standard certification entities such as SANS. Their retention with military service is critical due to the value they represent and the talent they bring to the fight. A person attracted to a military cyberspace operations position tends to typically have an introverted, analytical, and temperate personality. Many cyber professionals prefer to avoid being in the limelight and will even avoid being recognized for their outstanding performance. Performing within a leadership role is often an uncomfortable position for many in the cyber industry. Future leaders serving exclusively in the cyber branch will provide a more comprehensive understanding of operations, greatly benefiting our future leadership potential. How do we undertake the development of the leadership skills of our junior professionals giving rise to the future?

After extensive interviewing of the personnel at Detachment Texas, the consensus amongst all ranks is that the establishment of a technically exclusive path for our personnel to follow will give highly skilled technicians a path to progress within the ranks while still doing what they love. Personnel would be able to progress based on their technical skills and be compensated for the level of work they are performing. Retention in the cyber field would improve, helping to keep talented and valuable technicians in the ranks.

Having a purely technical path presents challenges with future leadership in a field that attracts a great deal of introverted personnel. Leadership is a crucially valuable trait in any organization. Detachment Texas feels that promotions come too rapidly within the cyber realm to properly train and prepare adaptable and flexible leaders. Tried and true tactics leaders use to groom their subordinates are difficult to pursue due to rapid promotion rates, our working environments, and a fast OPTEMPO. Many feel leadership potential should be measured and used as a qualification to follow a leadership path. Leadership potential could be tracked and improved similar to any of the other ASVAB aptitude scores. The development of leadership ability and traits seem to be something that we don't give a high enough priority. We could create or use partnerships with colleges to develop courses to build upon desired leadership traits.

Creating two distinct paths, one technical and one leadership, would allow Soldiers to pursue a career of their choosing while simultaneously benefiting the cyber career field by retaining talented individuals. Cyber would benefit as a whole to have a path for valuable and talented cyber professionals to follow that have little interest or intention to pursue leadership roles. By focusing on leadership development for cyber professionals who show an interest in leadership, we could prepare them more thoroughly ultimately benefiting the future of the branch.

FORT SAM HOUSTON, Texas *- Soldiers from Detachment Texas, 782nd Military Intelligence Battalion (Cyber), lead by 1st Sgt. Edward Maschek, hold their formation at the Quadrangle on Fort Sam Houston. (U.S. Army Photo)*

Learning from Innovation: Russian Information

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

Innovation is critical to successful cyberspace operations; fighting and winning in the cyber domain requires agility and an adaptability. Few would disagree that our innovators must be identified, encouraged, and empowered to drive change. However, one misconception with innovation is that it requires original thought on the part of the innovator. To the contrary, many well-known innovators have simply identified someone else's good idea and successfully implemented it.

German General Heinz Guderian, one of the pioneers of Blitzkrieg and modern combined arms warfare, became famous and successful for ideas that were not wholly his own. Guderian was heavily influenced by a British officer and strategist, J.F.C. Fuller. Guderian was so inspired by Fuller's innovative writings that he used his own money to translate them into German for his forces to study, and even invited him to attend German maneuvers before the World War II. Guderian's successful innovation, in no small part due to integration of Fuller's ideas, led to stunning successes on the battlefield. The German army conquered France in six weeks, a task they had been unable to accomplish in over four years during World War 1.

Fuller is less well remembered. He was unable to successfully execute many of his ideas within the British Army, and his abrasive personality almost guaranteed that any similar British innovation would fail.

Guderian is remembered as an innovator even though many of his innovations were not original thought. Fuller is little more than a historical footnote.

Knowing that we can, and should, learn from the experiences of others, Soldiers who fight in the cyber domain must constantly be on the lookout for innovative ideas expressed and executed by others that we can adopt or use to shape our own operations. One such example is on-going Russian innovations in information warfare.

Russia has openly discussed the development of "information confrontation" capabilities for years. Although U.S. doctrine writers acknowledge the importance of information, the military has struggled to effectively operate in the information domain. Changes in technology have only exacerbated the problem. As the Department of Defense seeks to transform the way we conduct operations in the information environment, Russia's experience offers many lessons. By examining Russia's treatment of information and information warfare, information warriors and leaders can gain valuable insights to apply to future operations.

What is Information Confrontation?

In 2013, Russian Chief of the General Staff, Valery Gerasimov, articulated a transformation in Russian military operations. Gerasimov was convinced that the West, led by the United States, had mastered modern warfare and was using it globally to great effect. He believed that the West was successfully using information confrontation to achieve both political and military objectives. Gerasimov's direction to the Russian military was anything but subtle, and three years later, nearly every article in Russia's premier strategic journal, Military Thought, discussed "New Type Warfare." New Type Warfare emphasizes the role of "non-military means" to achieve political and strategic goals.

Russian information confrontation includes both technical and psychological approaches; together they can degrade an opponent's combat power by creating chaos in the opposition.[1] Technical information confrontation includes enhanced electronic warfare capabilities and cyber warfare, changing the focus of war from ground combat to non-contact warfare. Psychological information confrontation allows Russia to shape both leader and population perceptions to subvert or paralyze opposing states.[2] Russian leadership believes

Confrontation

that controlling and shaping information can influence public consciousness. Although Russia cannot change facts or create a true alternate reality, information confrontation can generate enough fog and friction to prevent a timely, unified response. Both Ukraine and Syria have provided Russia a proving ground for testing information confrontation concepts.

If the Russians Copied Us, then Why Change?

Although information confrontation was born out of Russian perceptions of Western warfare, the U.S. military has significant room for improvement in the information space. For all the discussion about winning hearts and minds and recognizing that conflicts aren't about just enemy casualties, information has long been a sideshow in Joint operations, relegated to the Commander's special staff and subordinate staff elements.

The Chairman acknowledged this shortfall in 2017 when he added "Information" as the seventh Joint Function. Joint Functions are groupings of related capabilities and activities used to facilitate planning and employment of the Joint Force.[3] This addition raised Information to the level of the other Joint Functions, which includes command and control, intelligence, fires, movement and maneuver, protection, and sustainment.

The Joint Staff identified three reasons for establishing Information as a new Joint Function.[4] First, technology, particularly the Internet, changed how the Joint Force perceives and processes information. Second, our adversaries employ information in innovative ways that create vulnerabilities into the Joint Force. Finally, the vast majority of conflicts now conclude when the enemy decides to concede rather than relying on total and physical destruction. Defeat is often a cognitive outcome, with information playing a decisive role.

Fortunately, developing and refining information warfare can build on lessons learned not only from the U.S. experience in the domain, but from others as well. Russian operations and doctrine provide an approach to evaluate – and emulate when appropriate – and identifies capabilities required to counter Russian information confrontation. When examining Russia's experience in the domain, there are four clear lessons that should inform our own transformation towards information warfare.

Lesson 1. Information is a critical enabler in pursuing strategic and military objectives. Russian operations in Ukraine show that effective use of information and disinformation can play an essential role in creating strategic effects. For U.S. operations, information must enable the Joint Force Commander to maintain the initiative, and prevent adversaries from generating an effective response.

Russian information confrontation pursues two ends to force an opponent to relent: first, to create confusion; second, to cause internal turmoil. Both ends are used to achieve military objectives by complicating or shaping adversary decision making and disrupting a political unity of effort. Effective information confrontation puts adversaries "into a defensive posture and off balance, and thus, create conditions for surprise."[5]

Since 2014, Russia has waged information confrontation in support of operations in Ukraine to great effect. Information confrontation and its ability to create a fog of uncertainty allows the use of conventional military force outside of international norms while avoiding most strategic-level fallout. In Ukraine, information clearly supports Russian strategic, national objectives. Specifically, Russian policy indicates that a pro-Western government in bordering Ukraine threatens internal stability – one of six key Russian national interests.[6] To mitigate the risk of a Western sponsored revolution in Russia induced in Ukraine, Russia desires to either create a friendly government, or failing that, prevent a non-friendly government from establishing meaningful ties to the West. To establish a friendly government, Russia could possibly change the Kiev Government by force, or coerce them to take leadership from Moscow.[7] Alternatively, they could prevent stabilization of Ukraine's internal situation to avoid the emergence of a Western-leaning government. Russian chose to induce a crisis that precludes a Ukrainian move toward the West.

Continued on page 39

Cyber Swiss Army Knife

By 2nd Lt. Shane Neal, 915th Cyber Warfare Support Battalion

Introduction

While cyberspace and electronic warfare operations continue to proliferate through the Army, the demand for rapidly deployable Cyber and Electromagnetic Activities (CEMA) capabilities will persist. Support from Combat Mission Teams and CEMA professionals is limited across the operational force, which leaves a gap in the potential CEMA holds in multi-domain operations. The solution to this may lie in the thoughtful implementation of COTS (commercial off the shelf) technology into an all-encompassing CEMA platform. The vision is a man-packable system that operates independently of support by a cyber operator, is capable of cyberspace and electronic warfare operations, and promises integration of future development.

The Promise of Relevance

To remain relevant in cyberspace operations and adapt to any operational environment, the platform needs to offer a software solution that can be effectively handed-off between developers. It is unrealistic that a single engineering team would perpetuate as the main design-effort for the life of the system. A solution to this issue may be offered through an API (Application Programming Interface). An API would allow developers to rapidly build or modify capabilities without understanding the intricacies of the system's architecture or development stack. Additionally, over-the-air (OTA) updates would allow dynamic reprogramming of all devices, anywhere in the world. Instead of a black-box that is tailored to outdated technology, this concept promotes a modular platform that can be customized to any operation.

Technical Considerations

Software defined radios (SDR) may offer a viable solution in the development of a tool that supports cyberspace and electronic warfare operations. Typical radios are limited to the range of frequencies that their hardware is capable of modulating and demodulating to operate on the electromagnetic spectrum (EMS), consider for example Wi-Fi operating on 2.4GHz. However, SDR offloads the signal handling from hardware to software, enabling frequency ranges of 10MHz to 6GHz on a single system. Additionally, SDR receivers are commercially available, modular, and can be made inexpensive by pairing with other COTS technology like Raspberry Pis. As this programmable radio technology has already proved successful in disrupting UAS, it can certainly be incorporated into targeting other RF emitting devices.

Operational Vignette

Since the goal is to implement these all-encompassing cyber platforms in the operational force, compatibility with existing technology (driven by the API) is paramount. Consider for example, each Stryker in a Stryker Brigade Combat Team (SBCT) outfitted with one of these devices. The SDR would allow for a mesh network to be constructed between all friendly vehicles, providing a clear operational picture of friendly forces to the Combatant Commander and enable communication between each vehicle. Each platform could be equipped with software to actively conduct C-UAS with the mesh network ensuring that distributed computing is managed between each system, so no single device is overloaded. Additionally, the systems may be autonomously running directional finders to provide Soldiers in the field with enemy locations and provide remote operators a heat-map of network devices. Meanwhile, remote operators could roll-out a tool update to each device that actively disrupts enemy navigation and communication systems.

Closing Thoughts

While this 'Cyber Swiss Army Knife' does not exist in a single platform, teams are actively working to bring prototypes and existing capabilities under one hood. The 915th CWSB is actively working on capability development while understanding operational requirements from Corps and Below. With the right sourcing of time and talent, a single solution to cyberspace and electronic warfare operations in the field may be more than a lofty concept.

Guard Soldiers use innovative ways to improve fitness

By Maj. Shannon M. Machmiller, S2/S6, Task Force Echo 3, U.S. Army Cyber Command

NORMANDY, FRANCE *– Sgt. Colton Williams, Spc. Christopher Stafford and Capt. Thomas Sullivan (pictured from left to right) after completing the GORUCK D-Day 75th Anniversary Rucking Challenge in France, July 9. (Photo courtesy of Capt. Thomas Sullivan)*

FORT GEORGE G. MEADE, Md. – The mobilized National Guard Soldiers of Task Force Echo (TFE) are taking advantage of the opportunities offered in the central Maryland area to maintain and improve their physical fitness levels.

While there are plenty of fitness centers on Fort Meade and in the surrounding areas, many TFE Soldiers are finding innovative ways to increase their fitness. From completing in the Tough Ruck at the Boston Marathon, the Hike Across Maryland (HAM), GoRuck event at the D-Day Anniversary in France or training and competing in races such as the Army Ten-Miler, Soldiers are improving their fitness levels, building comradery and ultimately showcasing the essence of the National Guard Soldier.

A few Soldiers have even gone as far as creating their own group known as the Pirate Radio Ruck Club (PRRC), open to all ranges of experience. According to the Spc. Christopher Stafford, the PRRC founder, the group enjoys "working out regularly aiming for increasingly awesome (difficult) GORUCK events, to get a good sweat, walk, and conversation in." The group's end goal is to complete the Veteran's Day GORUCK HTL, which will take place in Washington, D.C. on November 9, 2019, to honor those who have served by those who are serving.

BOSTON *– Capt. Thomas Sullivan crosses the finish line at the Tough Ruck in Boston, April 14. (Photo courtesy of Sgt. Colton Williams)*

NORMANDY, FRANCE *– Sgt. Colton Williams (left) and Spc. Christopher Stafford during the GORUCK D-Day 75th Anniversary Rucking Challenge in France, July 9. (Photo courtesy of CPT Thomas Sullivan)*

Cyber Soldiers participate in Missing Persons

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

FORT BENNING, Ga. – *(from left to right) Staff Sgt. James Hansen, Staff Sgt. Joseph Rosales, Staff Sgt. Jackson Rolf, and Capt. Mark Klink, from the 100 Combat Support Team, E Company, 782nd Military Intelligence Battalion (Cyber), formed a four-person team to participate in the Trace Labs Global Missing CTF (Capture the Flag) 2 event, an Open Source Intelligence (OSINT) CTF for Missing Persons on July 13, and took third place out of approximately 100 teams. (U.S. Army Photo)*

FORT GEORGE G. MEADE, Md. – Soldiers from the 100 Combat Support Team, E Company, 782nd Military Intelligence Battalion (Cyber), participated in the Trace Labs Global Missing CTF (Capture the Flag) 2 event, an Open Source Intelligence (OSINT) CTF for Missing Persons on July 13, and took third place out of approximately 100 teams.

According to their website, Trace Labs is a "not-for-profit organization whose mission is to crowdsource the collection of OSINT to generate new leads on active missing persons' investigations…The CTF's purpose is to use OSINT tools and techniques to locate real missing persons around the world."

"The TraceLabs Missing Persons CTF is unlike any other CTF on the Internet," said Capt. Mark Klink, the 100CST team lead. "By using OSINT tools and techniques, competitors submit information (instead of flags) that is used by local and federal law enforcement agencies to locate real missing persons, missing from a matter of days to nearly 10-years. Due to the scope and the purpose of the CTF, a high degree of technical knowledge isn't required, and it's a good opportunity for the non-17 series (cyber operations specialists) members in our brigade to get experience competing in a CTF-like environment. In fact, many of our 35-series counterparts perform better in a CTF like this."

Competitors could participate as either a one- or four-person team. The four-person team from the 100CST included: Capt. Klink, Staff Sgt. Joseph Rosales, a cryptologic linguist (35P), Staff Sgt. James Hansen, a signals intelligence analyst (35N), and Staff Sgt. Jackson Rolf, a cryptologic cyberspace intelligence collector/analyst (35Q).

"Having no prior experience with CTFs, I didn't have an established set of OSINT tools going into this," said Rosales. "After the event, I believe we all came away better at gathering public information, which comes in handy not only for CTFs like this, but when it comes to my job as well."

"I was interested in competing because I saw it as an opportunity to sharpen some of my skills while contributing to a worthy cause," said Rolf. "Using OSINT tools should always be the first step when performing analysis, and I saw this event as way to learn new tools within the OSINT framework and improve my intuition during initial analysis."

In addition to be a worthy cause, Rolf highly recommends that other Soldiers participate in CTFs. "Analysts should have a good understanding of how to gather as much information as possible using open source tools because this is the least 'noisy'

Capture the Flag Event

form of information gathering. Participating in this event reinforced just how much useful information can be gathered on a subject using OSINT tools. I'd highly recommend that others participate in CTFs because they are great way to improve your analytic techniques, and they are a lot of fun."

Klink believes CTFs are an excellent way for Army Cyber and MI Soldiers, and Civilians, to stay sharp on tools and techniques they may not experience on a daily basis.

"Similar to crossword puzzles, Sudoku, Rubik's cubes, and other puzzles, CTFs allow individuals the opportunity to think critically and compete with peers, subordinates, and industry professionals all over the world," said Klink "In the case of the Trace Labs Missing persons CTF, nearly 100 teams submitted thousands of links to information regarding real-world missing persons information, including last known whereabouts, images, CCTV snapshots and more. This information is given directly to law enforcement agencies at the end of the CTF for use in locating the missing persons. Trace Labs tends to use the tag, #OSINT4GOOD, clearly stating that this CTF is "more" than your average competition, but directly contributing to the community and making the world a better place."

According to Klink, the CTF was very competitive, and although the event only lasted for eight hours "the fight for the top three changed pretty frequently up until about the last 60-minutes."

In total, there were nearly 100 teams and more than 200 individuals competing and the 100CST team, "Doing Great Things" came in 3rd place by a fair margin.

Klink remarked that it was the first time that two of the four people on their team had competed in any kind of CTF at all, and they certainly plan on competing next year at the next remote Trace Labs CTF, with the possibility of traveling to DefCon and competing at the 2nd Annual Trace Labs Missing Persons CTF at Defcon 2020.

"The competition was very competitive from the beginning. Our team had experienced analysts who were all taking it very seriously, and we still were unable to come out on top," said Rolf. "Our team was very much focused, breaking for only 20 minutes for lunch, during the eight-hour stretch of the competition. We came pretty close to breaking second place a few times, and I have no doubt that our team would have been neck-in-neck with first if we could do it again."

"The event was long, but knowing it was for a good cause kept me from taking many breaks," added Rosales. "I look forward to the next opportunity to compete in a CTF like this one."

The CTF was 100 percent virtual, so the contestants could participate from any geographic location, and although there was a minimal entry fee, all the proceeds went towards supporting the Trace Labs infrastructure and operating costs to enable the organization to continue crowdsourcing OSINT to assist in locating missing persons.

For more information on Trace Labs and upcoming CTF events, visit the Trace Labs Website at https://www.tracelabs.org/.

GLEN BURNIE, Md. *– 1st Sgt. Joel Aguilar, the senior enlisted leader for E Company (Empire), 782nd Military Intelligence (MI) Battalion (Cyber), 780th MI Brigade (Cyber), was recognized by the Rotary Club of Glen Burnie for his community service at the organization's "2019 Spring Fling: A Celebration of Service" banquet, May 3. (U.S. Army photos by Capt. Jacob Curtis)*

Cyber tool developer training is critical to the

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

FORT GEORGE G. MEADE, Md. – *The 780th Military Intelligence (MI) Brigade (Cyber) has partnered with the University of Maryland Baltimore County Training Centers in Gateway, Columbia, to design a Tool Developers Qualification Course (TDQC) which produces computer programmers for the U.S. Army. (U.S. Army Photo)*

FORT GEORGE G. MEADE, Md. – The 780th Military Intelligence (MI) Brigade (Cyber) has partnered with the University of Maryland Baltimore County Training Centers in Gateway, Columbia, to design a Tool Developers Qualification Course (TDQC) which produces computer programmers for the U.S. Army.

TDQC is an intense nine-month training program designed to meet the capability development requirements for the 780th MI Brigade and the most recent class graduated on July 26.

"TDQC is designed to train Soldiers who have little to no computer programming experience and after successful conclusion of the course, Soldiers are better equipped with the foundational knowledge and specialized skill to become a certified cyberspace capability developer," said Chief Warrant Officer 4 Tony Leota, the talent manager for the Cyber Solutions Development Detachment (CSD), 780th MI Brigade. "In other words, TDQC produces an Army computer programmer that will generate capabilities to defend the nation against enemies foreign and domestic in and throughout cyberspace."

Leota remarked that of the more than 270 Soldiers who have applied for TDQC, the course organizers selected 72 students and graduated 67. "This class marks the sixth TDQC iteration and these graduates join other TDQC alumni in expanding the Army developer community and establishing the foundations of this emerging cyberspace work role."

Lt. Col. W. Michael Petullo, a cyberspace operations officer and the lead developer for the CSD, was the host and guest speaker for the event. Petullo used his time to challenge the graduating class.

"Mentally prepare yourself for the challenges coming your way. You do this because you are now asked to make an impact beyond yourself. Grades are important. Being an honor grad is truly an honor, but these things derive meaning only from the service which follows," said Petullo. "Grades neither provide a capability to a mission team nor do they save American lives from bomb-carrying drones, but you will if you apply what you have learned, work with others in the cyber force who are different than you and their talents, maintain a perspective beyond your own work space, and fight through the challenges that inevitably arise in large organizations tasked to do large things."

Petullo remarked that the Army needs two people, "the current you, a TDQC graduate, and the future you, whose contribution and future growth is yet to be known." He said TDQC educates students, but it doesn't train them.

"When we teach you about concurrency models or threading, we expect that this will allow you to later adopt particular and new technologies as they arise," added Petullo. "Specific threading libraries,

Army's success

such as POSIX threads or Windows threading, what Hoare (Sir Charles Antony Richard Hoare is a British computer scientist) calls "communicating sequential processes" as so on."

Petullo then told the graduating class what common trait he has seen among all successful tool developers.

"I have administered a number of basic- and senior-level exams and I've watched 26 developers pass that later senior exam," said Petullo. "The developers that perform the best on this skill level exam have something in common. In fact it's the same characteristic that I found in my best computer science students during my four years as an assistant professor at West Point. The best developers have an intolerance for not understanding how something works. Indeed this is a cornerstone of the hacker ethic."

Sgt. Alan Kim, is a 35Q, a cryptologic cyberspace intelligence collector/analyst, who hails from Little Neck, Queens, New York, and is assigned to the Headquarters & Headquarters Company, 780th MI Brigade (Cyber). Kim has a Bachelor of Science degree in computer engineering from the State University of New York at Binghamton, and was the TDQC Distinguished Graduate.

Kim volunteered for the TDQC training for a myriad of reasons. "I took the course because programming is an interesting skill and it was a challenge."

Kim remarked that programming and computer engineering are two different disciplines and believes that programming is "at a higher level". He also felt that the TDQC course work was very difficult.

"When this (TDQC) opportunity came up I went for it and worked hard through it. The instructors provided the requirements and we had to code it to their standards."

Sgt. Nicholas Camp, is a 17C, a cyber operations specialist, who hails from Rochester, New York, and is assigned to the Cyber Protection Brigade's Development Group. Camp is in his junior year at Dakota State University and is pursuing an Associate's degree in Network Infrastructure Security, and eventually a Bachelor's and Master's degree in Cyber Security. He was the TDQC Honor Graduate.

Although Sgt. Camp had already reenlisted, he extended his enlistment for an additional three months, specifically to attend TDQC, because he wanted "to better my experiences to prepare myself for a work role in cyber that's going to be a little more stringent on learning and provide a competitive edge to combat our adversaries. It makes it more challenging to find a programmatic way of finding issues rather than doing it manually."

Camp believes that following TDQC he has "a great foundation to build upon and continue to grow as it is forever a learning experience."

Kim and Camp both thought the course was very challenging and wanted to express their gratitude to all of the UMBC instructors, especially Liam Echlin, the lead instructor at the UMBC Training Centers.

"TDQC is a great opportunity for enlisted Soldiers because it gives those of us with degrees or want to get degrees to be at a higher spectrum in education. It's also an opportunity to push ourselves, intellectually," said Camp.

Camp said Soldiers who are preparing to take the TDQC pre-test should know the basic coding concepts.

"Not a particular language, just basic coding concepts, because they are the same throughout," said Camp. "In preparation, you need a mindset of how code operates, thinking about things sequentially and broken down into small steps is hugely important since we normally don't think that way."

"If you were to look up 'coding concepts', you can definitely find it," added Camp. "There are books that you can get for free, a lot of e-books that will explain it."

The 2019 TDQC graduating class includes: Sgt. Nicholas Camp; Chief Warrant Officer 2 Christopher Charland; Spc. Ryan Jonassen; Sgt. Alan Kim; Sgt. 1st Class Matthew Longwell; Staff Sgt. Samual McCracken; Spc. Taylor Morse; Sgt. 1st Class Christopher Naugle; Spc. Cody Reed; Sgt. Kristin Rierson; Spc. Jacob Sevy; and Spc. Scott Wareham.

Congratulations to each of the 2019 TDQC graduates, and welcome to the world of capability development.

Enemies and Allies of Innovation

By Frank Colon, Cyber Operations Attorney, 780th Military Intelligence Brigade (Cyber)

Frequently, the phrase "legal said no" appears to put the legal office as the eternal enemy of innovation. Sadly, this is true in many legal offices, but not ours. I can count on one hand the number of times I said "no" in over 21 years of active duty and five years as a civilian attorney. I propose the statement "legal said no" is fake news. Most of the time legal says maybe, or I think so, and after a few more questions, some research, and maybe a few adjustments to the plan, legal says "yes".

Why does this apparent disconnect exist? The reason is legal, along with other disciplines, must ensure the innovation complies with standards and controls, applies best practices, and minimizes waste and errors. By doing so, we help put armor on the innovation so it survives first contact with the real enemy of innovation – bureaucracy. Although creativity and innovation necessarily involves exploring sometimes radical or unorthodox ideas, deviating from existing standards and controls can cause risks that doom the project to failure if not done deliberately and with great care. Our goal is to identify issues with proposed innovations so that they can make it past the front door of the Brigade Headquarters. Therefore, legal and innovation can cohabit in the same Brigade and work together to provide armor to the innovation. Armor insulates the innovation from bureaucracy.

IBM did the same when they had small "skunkworks" teams compete to develop the Personal Computer. Don Estridge and a team of 12 engineers in Boca Raton, Florida, in just 18 months built a prototype, gained approval and launched the project which redefined the market and set the new standard for PCs. Of course, without this innovation, none of us would be now working in an offensive cyber brigade.

A successful organization like ours can focus on innovation, but must ensure the idea is able to take its first breath and have sufficient armor (standards, controls, and best practices) before it leaves the front door. Creativity does not mean chaos nor does it mean leaving things to chance. You can put in place processes for idea generation, idea evaluation and proposal implementation. The whole process can be managed while accepting many formal and informal inputs. Innovation succeeds when a whole of Brigade approach is used from idea, to plan, to review, to deployment, converting ideas into valued outcomes.

FORT GEORGE G. MEADE, Md. *– Col. Brian Vile, commander of the 780th Military Intelligence Brigade (Cyber), leads the brigade on a three-mile run during the installation's All-Services Birthday Commemoration Run on June 14, which is consequently the U.S. Army's 244th Birthday. (U.S. Army Photo)*

Lessons learned and Safety Tips to Preventing Carbon Monoxide Poisoning

By Brian K. Sylvester, Safety Specialist, 780th Military Intelligence Brigade (Cyber)

This invisible killer, kills without any notice: CO2. An odorless and colorless gas that often goes undetected, striking victims caught off guard or in their sleep. When we wake up each day we probably would never think about this invisible killer taking our life or the life of a loved one or co-worker. In fact, we most likely never think about it as we roll of out of bed and crawl to the kitchen to start the coffee maker for that fresh brew. But we need to think about it!

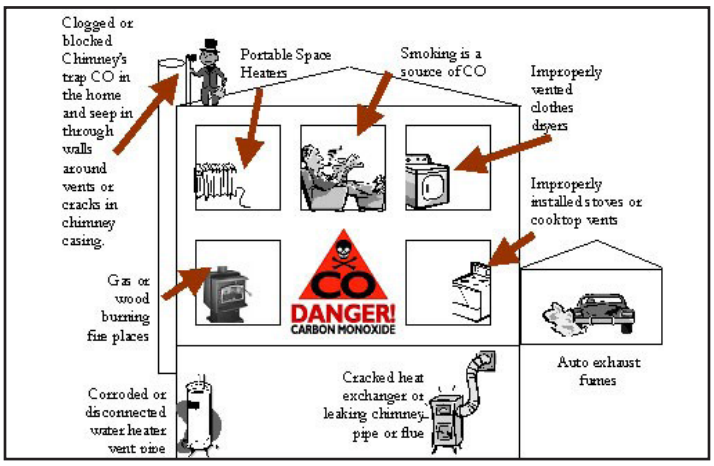
According to the Centers for Disease Control and Prevention, more than 400 people in the U.S. die from unintentional CO2 poisoning every year, with more than 20,000 emergency room visits, and more than 4,000 others hospitalized.

Lessons learned from CO2 Accidents

Have you ever thought about this – If you are in the market for a new car, you will find that all newer models are equipped with keyless entry: An easy push of a button starts your car just as long as you are carrying the fob. This feature can become a contributing factor to an accident that results from human error. The story normally starts and ends like this: Victim parks car in garage, forgets to turn car off by pushing keyless start, and later CO2 strikes! A horrific example of this occurred in 2015, when a man succumbed to CO2 after leaving his car running in a garage attached to the home. Unknown to the victim that the car was still running, he fell asleep with the key fob in pocket. He never woke up.

In another example, the Department of Labor reported that two landscaping employees died from CO exposure after a gasoline-fueled lawnmower was started inside an enclosed company trailer that then transported the crew to a jobsite. Not only did the company expose its employees to the deadly gas, but it failed to train employees to recognize the hazard to begin with.

Accidents such as these could have been prevented through proper hazard identification, assessment, and mitigation.



Identifying the hazard

The bad news is that anyone can be at risk. However, the CDC says infants, the elderly, and people with chronic heart disease, anemia or breathing problems are more prone to illness or death. The good news is that this "invisible killer" is produced by burning fuels that can be detected before it is too late with appropriate safety measures. Cars, fireplaces, gas ranges, portable generators or furnaces burn this fuel.

Winter can be a prime time for carbon monoxide poisoning as people turn on their heating systems and mistakenly warm their car in garages so please take extra precautions to ensure safety.

So how you can we prevent CO2 poisoning?

The National Safety Council recommends that you install a battery-operated or battery backup carbon monoxide detector in the hallway near each separate sleeping area in your home. Check or replace the battery when you change the time on your clocks each spring and fall and replace the detector every five years. If the carbon monoxide alarm sounds, do not ignore it and do not attempt to find the source of the gas. The Consumer Product Safety Commission instead recommends following these steps:

- Immediately move outside to fresh air.
- Call Emergency services, fire department or 911.

Continued on page 45

God: The Greatest Innovator

By Chaplain (Capt.) Mike Cerula, battalion chaplain, 781st Military Intelligence Battalion (Cyber)

"…by God's word the heavens existed and the earth was formed out of water and by water (2 Peter 3:5)."

I believe that this universe was created and filled with designed intelligent beings, each containing a number of systems of irreducible complexity. Not everyone believes this.

Charles Darwin held firmly to the belief that a great number of variations, from imperfect to perfect, resulted in the complex human eye. By his own admission, this seemed absurd.

"To suppose that the eye with all its inimitable contrivances for adjusting the focus to different distances, for admitting different amounts of light, and for the correction of spherical and chromatic aberration, could have been formed by natural selection, seems, I freely confess, absurd in the highest degree."[1]

Still, he held to his conclusion that the eye generated its complexity on its own.

Another scientist, Wernher von Braun, in his 1972 letter to the California State Board of Education, felt convinced our eye was uniquely special.

"The better we understand the intricacies of the universe and all it harbors, the more reason we have found to marvel at the inherent design upon which it is based… What random process could produce the brain of a man or the system of the human eye?"[2]

Our eyes are not the only thing of note within our bodies. There are many fascinating objects to study. Life has complex machinery even on a micro scale, such as the flagellar motors on bacterium. Even an article against intelligent design describes its complexity.

"In E. coli, [directing movement] works by changing flagella rotation from anticlockwise to clockwise and back again, causing a cell to tumble and then head off in a new direction."[3]

Without acknowledging a Great Innovator who would create all parts of this machine simultaneously, we're left to conclude that certain proteins had to wait on the rest to show up and somehow remained functional, or knew to wait.

We have great 'highways,' that transport precious life-giving cargo. "[Our circulatory system] - is over 60,000 miles long. That's long enough to go around the world more than twice!"[4]

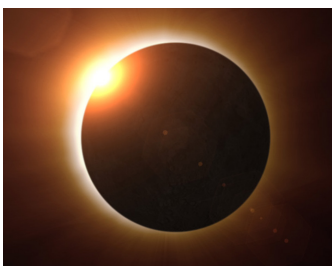
The human genome (our complete DNA) has about three billion base pairs.[5] The letters of this genome need to be organized sequentially, which just like any other organized language, speaks to me of an Intelligent Being.

For the cyber Soldiers and civilians among us, it is neat to point out that humans even come complete with a supercomputer! "…the human brain probably contains more than 1014 synapses."[6] Has anyone designed a computer that can match that?

We have abilities that natural selection fails to adequately answer. Our stomach acid is capable of dissolving metal.[7] Yet, its epithelial cells simultaneously secrete mucus to protect itself.[8] And the epithelium lining stays fresh, regenerating itself every 5-7 days.[9]

I find that unlikely symbiosis of harsh acid and soft lining to be rather spectacular.

But as practical as much of this seems, I believe God also designed some things for our enjoyment- like the total solar eclipse. After crunching the numbers, the diameter of the sun is just about 400 times larger than Earth's moon. Yet, the moon is an average of 390 times closer to the Earth. That incredible 'coincidence'



Continued on the next page

results in wonderful total solar eclipses, revealing just the sun's corona.[10]

Even our planet points to an innovative design. We are on a unique planet, compared to any other ever known or found, something Dr. Hugh Ross' book, The Creator and the Cosmos, comprehensively outlines. Consider this:

"The rotation period of a life-supporting planet cannot be changed by more than a few percent. If the planet takes too long to rotate, temperature differences between day and night will be too great. On the other hand, if the planet rotates too rapidly, wind velocities will rise to catastrophic levels. A quiet day on Jupiter (rotation period of ten hours), for example, generates thousand mph winds . . ."[11]

The same precision must also occur with our planet's axis. Our axis tilt prevents exceedingly harsh hot and cold temperatures from plaguing our pale blue dot. Our atmosphere is comprised of just the right mixture of oxygen, nitrogen, and carbon dioxide to sustain life as we know it. Earth comes complete with a vibrant magnetic field necessary to guard against cosmic radiation.

Consider the word of this scientist, who knew a thing or two:

"This most beautiful system of the sun, planets, and comets, could only proceed from the counsel and dominion of an intelligent and powerful Being." -Sir Isaac Newton[12]

Friend, you are fearfully and wonderfully made (Psalm 139:14) by a loving God and Creator. You yourself are unique and unlike anyone else in the entire universe, no one has your fingerprints! Just know that everyone has at least one gift to offer and is of priceless worth! Your life matters! Please consider that you were made for a reason. In the words of Gianna Jessen, abortion survivor, "Don't you realize, you cannot make your own heart beat… it is the mercy of God that sustains you, even when you hate him."[13]

No matter what inventions we design or what solutions we generate, God will always be the original and greatest innovator. Nothing humankind has ever made can compete with the Creator's work.

---

1 Darwin, C. (1859). On the origin of species by means of natural selection, or the preservation of favoured races in the struggle for life (pg. 186). London: Murray.

2 San Diego Reader. (2012, July 18). Retrieved July 16, 2019, from https://www.sandiegoreader.com/news/2012/jul/18/excerpt-letter-california-state-board-education/

3 NewScientist. (2008, April 16). Retrieved July 16, 2019, from https://www.newscientist.com/article/dn13663-evolution-myths-the-bacterial-flagellum-is-irreducibly-complex/

4 Cleveland Clinic. (2019, April 30). Retrieved July 16, 2019, from https://my.clevelandclinic.org/health/articles/17059-how-does-blood-flow-through-your-body

5 National Human Genome Research Institute. (2018, November 12). Human Genome Project FAQ. Retrieved from https://www.genome.gov/human-genome-project/Completion-FAQ

6 Barnes, D. M. (1986). Brain architecture: Beyond Genes. Science, Vol. 233, 155.

7 Li, P.K., Spittler, C., Taylor, C.W., Sponseller, D., & Chung, R.S. (1997). In vitro effects of simulated gastric juice on swallowed metal objects: implications for practical management. Gastrointestinal Endoscopy, 46(2), 152-5. Retrieved from https://www.ncbi.nlm.nih.gov/pubmed/9283866

8 Smith, M. E., & Morton, D.G. (2010). The Digestive System (Second Edition). Retrieved from https://www.sciencedirect.com/topics/medicine-and-dentistry/mucus

9 Barbuzano, J. (2017, July 14). Understanding how the intestine replaces and repairs itself. The Harvard Gazette. Retrieved from https://news.harvard.edu/gazette/story/2017/07/understanding-how-the-intestine-replaces-and-repairs-itself/

10 NASA. (2019, June 12). Earth's Moon. Retrieved from https://solarsystem.nasa.gov/moons/earths-moon/in-depth/

11 Ross, H. (2001). The Creator and the Cosmos (pp.135-136). Colorado Springs, CO: NavPress.

12 Newton, I. (1846). Newton's Principia the Mathematical Principles of Natural Philosophy [First American Edition] (pg. 504). (A. Motte, Trans.). New York: Daniel Adee. (Original work published 1687)

13 Jessen, G. (2008, September 8). Gianna Jessen Abortion Survivor in Australia Part 1 [Video file]. Retrieved from https://www.youtube.com/watch?v=kPF1FhCMPuQ

Inspiring Innovation

By Chaplain (Capt.) Kevin White, battalion chaplain, 782d Military Intelligence Battalion (Cyber)

I have been the Cyber Legion Battalion Chaplain since July 2017, and I have been in awe of the creativity and innovation exhibited from day one. I have had the privilege of watching our OPTEMPO (operation Tempo) continually increase due to increased demand for what we offer because of the hard work and determination of our teams. As everyone in the 780th Military Intelligence (MI) Brigade continues to meet every new challenge head on, we prove how important cyber is to the overall success of our National Defense. If you are reading this, you are a part of that, and isn't that amazing?! As I watch, listen, and encourage, I hear amazing stories from every level about new problems and innovative solutions. Innovative thinking is a major contributor to the greatness of our Army, and innovation is certainly in the DNA of the 780th MI.

But what can a Chaplain add in the midst of all these great minds? I certainly cannot help with coding! However, it is my assertion that our core "programming" is imbued with innovation. The first story in many religions, is a creation story. The Jewish and Christian Scriptures begin with, "In the beginning God created the heavens and the earth. The earth was formless and void, and darkness was over the surface of the deep, and the Spirit of God was moving over the surface of the waters" (Genesis 1:1) Creativity is at the heart of who God is, and according to Genesis 1:27, "God created [humanity] in His own image, in the image of God He created [them]; male and female He created them." Therefore, when we exercise our innovative imaginations in order to overcome obstacles, we are accessing the creativity that is at the heart of the human source code. We are created to innovate.

Furthermore, as beings created in the image of God, we are created to be in relationship. The Hebrew Word translated "God" in Genesis 1, Elohim, is plural. The traditional Christian worldview upholds the doctrine of the Trinity—there is one God manifested in three persons (Father, Son, and Holy Spirit) existing in perfect relationship. Genesis 1:26 begins, "Let Us make [humanity] in Our image…"

Our humanity is best expressed in relation to others, and it is through relationships (family, friends, teams…) that our creative potential is maximized.

You are an example of that maximized creative potential. The amazing things that were accomplished since the inception of our great Brigade, the awesome work being done right now, and the yet unheard of innovations to come are proof that we are all "fearfully and wonderfully made" (Psalm 139:14). Therefore, I thank you for encouraging me with your inspiring innovation.

Steward through Innovation

By Sgt. 1st Class Paul Peterson, Equal Opportunity Advisor, 780th Military Intelligence Brigade (Cyber)

Greetings Praetorians! This quarter's topic, innovation, has really struck a chord with me and I am excited to share my thoughts and my take on such a powerful tool. Innovation is why we are able to do so many amazing things in today's modern military. Just that phrase alone, "modern military", implies innovation. Why are we modern? Why are we able to be a military? Innovation is why. When you go to the range, you aren't using musket are you? The military's transportation doesn't still rely on horses, does it? Do you still stand toe-to-toe with your enemies on the grassy hill? No. As stewards of the profession we have taken leaps of faith in leveraging technologies and partnerships to innovate newer, greater, and more effective means to fight and win our nation's wars. In this article I hope to impress upon you the need to look for the opportunities around you and the environment you operate in to seek out ways YOU can be the front runner of innovation in your organization.

As the Equal Opportunity Advisor of the brigade I get to talk to many of you one on one or in small groups. One resounding theme I see and hear often is a concern for lack of leadership opportunities. I would encourage you to innovate. We do not have the same force structure as other types of Army units, however, leadership is not solely an Army function. The Army would love to hear all about how you successfully trained, mentored, and led your team into battle. It also understands this is not the case for many of our leaders. I would encourage you to look beyond the conventional ideas, and go to your civilian peers. Many academic institutes could use your aid. There a plethora of youth and adults alike who could benefit from the insights a Soldier could bring them. Start a working group, quarterly seminar, training event, or any collaborative effort focused on positive influence. You just might find yourself cultivating a long-lasting relationship with a new recruit, sprouting organization, or building a new process fostering military and civilian relations. It takes you, the leader, to take the first step towards success. It takes you to have the vision, share it with those capable of executing, and see it through. Leadership is not a position folks. It's a mindset!

While preparing to host the LGBT Special Observance this June, I came across some other organizations who were finding their own way to celebrate our communities. The Stonewall Monument is a monument you can only see through your digital device using a camera. It is quite the spectacle! Upon seeing this my brain immediately went into the mode of "how can we use this?" I am no tech guru by any means, but I thought about how cool it would be if our Soldiers within the 780th could harness this type of technology for different purposes. This was innovation I was looking at. A new way to do something we have been doing for years. I can tell you in my over 15 years of service I haven't seen anything like this in the Army. Why not? You tell me. Can we do it? What would we use it for? These are questions I pose to you, the capable cyber leader. If the Army can embrace a simple stick figure video for its SHARP training, I am positive you can do better. Be the leader, innovate with the Army's best interests in mind.

In closing I want to thank you for your continued support to the Equal Opportunity Program. Our world, nation, Army, and teams are all changing. It takes a brave mind to embrace change. Change in all forms. The military has standards we all agreed to. We even agreed to the standards that will come in the future. Take a stand against unfair discrimination. I will be here to support you. If you have any questions, comments, or concerns please contact me and I will do my best to assist you with anything you need.

SFC PAUL PETERSON
780th MI BDE (Cyber)
BLDG 310 Chamberlin Ave
Fort Meade, MD 20755
Equal Opportunity Advisor
paul.m.peterson6.mil@mail.mil
Office: (301) 833-6412
Work Cell: (301) 974-2763

Building the next cyber generation at Meade High

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

FORT GEORGE G. MEADE, Md. *– 1st Lt. Conner Wissmann, the lead CyberPatriot mentor and battalion assistant S3 (operations), 781st Military Intelligence (MI) Battalion (Cyber), 780th MI Brigade (Cyber), is teaching high school students about cyber security at a CyberPatriot CyberCamp at Meade High School. (U.S. Army Photos)*

FORT GEORGE G. MEADE, Md. – Service members and Army Civilians representing U.S. Cyber Command (USCC) and the National Security Agency are teaching high school students from throughout Anne Arundel County Public Schools about the basics of cybersecurity this week as part of the Air Force Association (AFA) CyberPatriot CyberCamp at Meade High School. The event continues next week, August 5 – 9, with a focus on more complex cyber concepts.

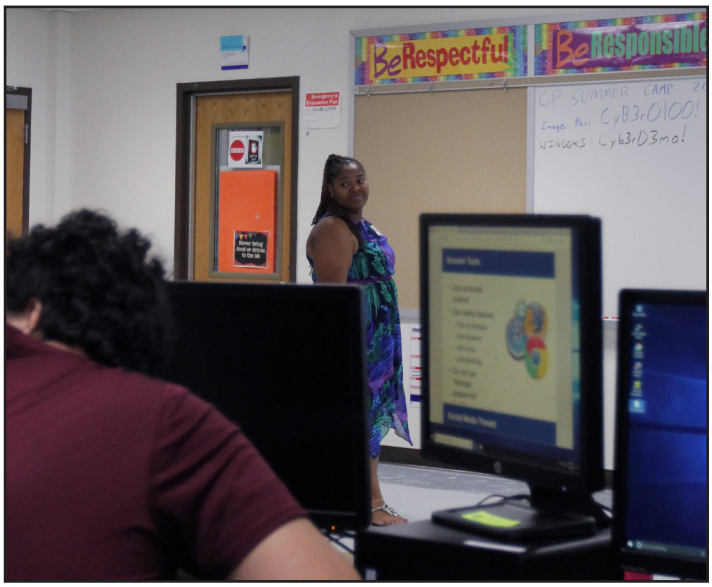
The Meade High CyberCamp began with an opening ceremony in the high school's media center and was attended by Maj. Gen. Timothy Haugh, commander of the Cyber National Mission Force, Master Gunnery Sgt. Scott Stalker, the senior enlisted leader for U.S. Cyber Command and the National Security Agency, Col. (retired) Peter Jones, the AFA Central Region president, Dr. Frederick Rivers, the principal for Meade High School, as well as several local state representatives and business leaders.

Stalker was the guest speaker and specifically addressed the CyberCamp attendees when he said, "In this environment, in cybersecurity, in STEM, all of the opportunities are out there."

"There will be times where it's hard, where it's challenging, when you might say 'I don't know what I've gotten myself into, this is not for me. Push through," said Stalker. "Grab a mentor, ask questions, persevere through, and I promise you on the backend, there are opportunities there. Whether you are creating the next version of Fortnite, creating your own company, or if you decide to walk across the street and work with us at the National Security Agency and United States Cyber Command, all of those opportunities will be there for you."

Justin Serota is a computer science resource teacher and DoDEA (Department of Defense Education Activity) Cyber LAUNCH Grant resource teacher for Anne Arundel County Public Schools, and works out of Meade High School. Serota said there are only three CyberPatriot programs throughout the county.

"CyberPatriot is a national competition, really a series of competitions, throughout the school year and the students learn how to secure images," said Serota. "They use virtual machines and they learn how to secure Windows, Ubuntu, and Linux machines. They learn all the basics of cybersecurity to include networking, cryptography, encryption, operating system basics, settings and password settings."



FORT GEORGE G. MEADE, Md. *– April Taylor-Melton, a CyberPatriot mentor and battalion IT specialist with the 781st MI Bn., is teaching high school students about cyber security at a CyberPatriot CyberCamp at Meade High School.*

Serota said CyberPatriot is an important program not only because cybersecurity is critical to national security, but also because of the career opportunities for those students that get involved.

"It's a very wide-ranging field and the students are not aware of these opportunities," said Serota. "CyberPatriot is a pathway to let them understand what they can do after high school and college."

Before the training began on the first day of CyberCamp, 1st Lt. Conner Wissmann, a cyberspace operations officer assigned to the 781st Military Intelligence (MI) Battalion (Cyber), 780th MI Brigade (Cyber), and the lead CyberPatriot mentor for Meade High School, cautioned the students about the dangers of computer hacking and malware, and their responsibilities when they get on a computer.

"When I get behind a computer the image that I've been given – the cyber student image – has tools on it that can do bad things to good networks, including the school's network. So, this is your code of conduct that basically says I will not do bad things to networks…bad things are those things that you shouldn't do," said Wissmann.

To emphasize the negative aspects of computer use, April Taylor-Melton, a CyberPatriot mentor and battalion IT specialist with the 781st MI Bn., and her colleagues discussed credit card skimming, cyber-bullying and recent cyber incidents such as the Equifax data breach in 2017, the compromise of T-Mobile customer data in 2018, and the recent ransomware attack on the City of Baltimore.

"I think there are two primary reasons for the students to be here," said Wissman. "One is for their personal gain. They won't get taught these things anywhere else, not in school, not at home…it is worth their time to be here."

"The second reason is to foster good digital citizens," added Wissmann. "We hear about these attacks and we had some lessons today where the students were presenting them to us. A lot of the cyberattacks are the result of bad digital hygiene or not understanding how computers work. Even if the student doesn't become excited or doesn't get into this field, they can still learn something that will protect them or their families, or society as a whole. It's exciting and that's why I volunteer."

According to Taylor-Melton, the computer classes

FORT GEORGE G. MEADE, Md. – *Daniel Sorensen, an analyst assigned to the 781st MI Bn., is teaching high school students about cyber security at a CyberPatriot CyberCamp at Meade High School.*

taught in schools usually focus on PowerPoint, Excel, the Microsoft Office services. Students are not taught about the operating systems or how to protect themselves.

"Even if it's for just these two weeks, the classes have given them much more than what they already knew," said Taylor-Melton. "Previously, they have never touched Linux, some of them have never even heard about Linux, and even when we had an operator come in here, a hacker, and tell them what he does, it provided them with a broader view of what cybersecurity is and what it can be."

The mentors were clear, however, that CyberPatriot was not hacker training, but rather a fun way to learn cyber security skills that would be useful to them in the future.

The CyberPatriot mentors: Wissmann, Taylor-Melton, Dan Sorensen, an 781st MI Bn. Analyst, Spc. Jacob Cochran and Sgt. Joshua Abraham, both from the 741st MI Bn., 704th MI Brigade, and CTN2 (Cryptologic Technician Networks) David Mason, Cyber Strike Activity 63, U.S. Navy Cyber Command, remarked that without the support of their chain of command, they wouldn't be able to volunteer.

"On Monday, at the opening ceremony, when Lt. Col (Nadine) Nally saw the three of us from the 781st sitting in those chairs, she realized if we weren't here there would be no CyberPatriot program," said Taylor-Melton. "Our commander realized how much time and effort we have put into this – I was going to take leave for two weeks to be here and she said

Continued on page 47

Russian Information Confrontation (cont.)

Continued from page 24

This crisis began with a Russian invasion of Crimea and Eastern Ukraine in 2014. During the invasion, information confrontation created confusion about facts on the ground in order to prevent a unified international response to the Russian invasion. These activities countered and obfuscated substantial evidence of direct Russian involvement in the war, including prisoner exchanges, deaths of Russian service members, and sightings of T-90 tanks and other sophisticated Russian equipment in Ukraine. Russia also successfully obscured the facts about their efforts by preventing Organization for Security and Co-operation in Europe observers from monitoring the cease-fire [8] and denying access to Malaysian Airlines Flight 17 (MH17) crash site, a civilian aircraft downed by Russian anti-air assets, for over two weeks.[9] Even Russian involvement in the downing of MH17 has been muddied, and many Western states remain reluctant to identify Russia or their proxies as responsible.

Despite having undeniably violated internationally recognized borders, Russia justified their actions by clouding the information domain. Moscow ignores facts that are contrary to their objectives. Instead, they characterize Crimea as part of Russia and actively undermine Ukrainian political leadership using inaccurate and incomplete information.[10]

At the strategic level, information confrontation was clearly successful; there has been a remarkable lack of international response to Russian misconduct. Despite the Russian delivery of weapons and their involvement in combat operations, some Western countries still deny that Russian forces have entered Ukraine. Of interest to our own transformation, this application of information confrontation was intended to enable military operations rather than achieve diplomatic or economic goals.

By following the Russian example and better integrating the Information function into U.S. operations, Joint Force Commanders can achieve strategic objectives. However, instead of using disinformation to obscure activities, Information must be used to provide clarity while being consistent with objective reality. Although fog and friction are useful at the operational and tactical levels, for Western democracies, they are counterproductive at the strategic level. As we press forward with developing and refining information warfare, we must remain true to our democratic ideals.

Lesson 2. Countering information confrontation requires empowering Commanders at all levels to seize the initiative. Russian operations in Syria show that Commanders must be proactive, timely, and transparent to successfully mitigate information confrontation.

Syria offers a second operational vignette for consideration. Russia's campaign to support the Syrian government employs information confrontation to gain a strategic advantage by obscuring facts on the ground, allowing employment of military force in a brutal manner, often against civilian and protected targets. Russia's elaborate information confrontation scheme has successfully protected their operations from significant international backlash.

The nexus for information confrontation efforts is the Russian Centre for Reconciliation of Opposing Sides in the Syrian Arab Republic,[11] which published daily reports on Russian and Syrian operations. These reports consistently asserted that Russia and Syria only attack terrorist organizations, despite clearly engaging a much broader target set. For example, on June 17th, 2016, two Russian Su-34s attacked coalition-backed forces in Syria; they only broke off the engagement when U.S. F-18s arrived on scene.[12] The Russian report for that day states, "Russian Aerospace Forces and Syrian Air Force did not make strikes on opposition armed formations which follow ceasefire regime and informed the Russian or American Centres for reconciliation about their location."[13] Although demonstrably false, Russian claims were frequently repeated by Western media, further obscuring the truth and distracting observers from reality.

Continued on the next page

Information is also used to obfuscate and distract from grave violations of international norms. Despite well-documented transgressions and violations, information confrontation limited and rendered irrelevant Western concerns regarding Russian military operations. For example, the Syrian Observatory on Human Rights identified 2,498 Syrian civilians killed by Russia in nine months of airstrikes through 2016 [14] – a rate ten times higher than that generated by coalition forces. [15] Moreover, there are legitimate claims that Russia deliberately targeted civilians and critical infrastructure in opposition-controlled areas. As a result of deliberate Russian targeting of hospitals, Medicines Sans Frontiers stopped co-locating their operations in opposition-controlled territory.[16] Reports also indicated Russia destroyed grain silos, markets, and water treatment plants.[17]

Despite the strength and magnitude of these charges, Russian disinformation blunted Western accusations of uninhibited, if not illegal, conduct in Syria. Furthermore, the West did not take meaningful action to curb Russian attacks. During the 2016 Munich Security Conference, Prime Minister Dmitry Medvedev audaciously said there was "No evidence of our bombing civilians, even though everyone is accusing us of this."[18]

From a military perspective, the neutering of any effective response allowed Russian forces to ignore civilian casualties and create humanitarian disasters to marginalize opposition capacity. Information capabilities allowed Russia to employ non-precision weapons in populated areas and engage in indiscriminate targeting, significantly simplifying offensive operations and enhancing the ability of their forces to defeat Syrian opposition.

Obviously, Western forces must not use information or disinformation to obfuscate mistakes and commit war crimes. Disinformation is an anathema to democracies, and the long-term adverse effect on military operations and reputation would offset the short-term gain. Instead, the Joint Force Commander must use Information to counter adversary misuse and exploitation. Successfully doing so requires advance planning and knowledge of friendly military operations and being prepared to respond quickly to inaccurate or incomplete information from our adversaries.

Planning for Information activities in joint operations is the easier of the two tasks; most major operations already consider and integrate Public Affairs. However, this approach could be seen merely as an attempt to spread propaganda. Shielding subordinate commanders from the press may allow them to focus on conventional operations, but loses an opportunity to provide timely, factual, and unvarnished information. In the information age, this trade-off no longer makes sense. Commanders at all levels must be prepared to provide ammunition to the information fight at the pace that strategic objectives demand rather than as an after-action activity, including in near-real time, if necessary.

Countering our adversary's information activities will remain difficult. Many of our adversaries, including Russia, traffic in disinformation and do so quickly and decisively. Disinformation requires no time-consuming fact-finding; creating a useful story not bounded by facts requires only a vivid imagination and a sharp tongue.

Successfully countering this disinformation requires an agility and transparency difficult to achieve in a connected and lighting fast technological world. Information and disinformation in modern society move in milliseconds, and stories rarely merit more than a day or two of attention. Unless the information is countered immediately, if can be impossible to control the damage. Doing so successfully will require Joint Force Commanders to execute mission command and empower subordinate commanders to directly respond to disinformation with verifiable, truthful information. With information confrontation, time is of the essence to effectively counter adversary messaging.

Lesson 3. The information environment is fast and fluid; there is little time for deliberation. Joint Force Commanders must consider not only the means and the insatiable demand for information, but also the pace at which the fight occurs. The complexity of the information environment will require reorganization of existing staff elements the development of new capabilities.

Russia demonstrated technology's transformation of the information landscape. In addition to the more traditional television and radio networks, the

Continued on the next page

Russian Information Confrontation (cont.)

Continued from the previous page

Internet and social media have become an essential part of information exchange activities. To take advantage of this change, Russia extensively financed information efforts and organizations, dedicating over $1.3 billion to state-run media alone.[19] Their state-sponsored primary media outlet, Russia Today (RT), operates with a $300 million budget.[20] Although it acclaims to present the Russian perspective, their reporting is often at odds with objective facts. For example, RT advanced speculative stories that flight MH17 was shot down by the North Atlantic Treaty Organization, despite a lack of forensic evidence to back up either case. Russia's Internet Research Agency, infamous for efforts during the 2016 U.S. elections, operates "troll farms," where hundreds of workers run false social media pages, post pro-Russian commentary on a variety of Internet sites and systemically attack opponents of Russia while promoting Russian institutions and methods.[21]

Russian information organizations present a constant flow of information in support of strategic objectives. For social media in particular, these organizations exploit the ability to "push" information to targeted audiences. Unlike television where users need to tune in, social media allows information practitioners to target audiences using hashtags and communities of interest while they check their daily email. Rather than having to look for information, social media can actively push information based on demonstrated or expressed interests. The profit motives of social media companies also enable pushing – ads can be targeted to specific audiences, identified based on search history analytics and associated data, for a price.

This environment provides the Joint Force Commander the ability to quickly and accurately disseminate information to targeted audiences and counter adversary disinformation. Commanders need robust capabilities to automatically identify and track information and disinformation related to the Joint Force operations. Technical identification of an on-going information fight is only part of the battle. Once identified, commanders at all levels must be prepared to respond immediately with facts. To preserve lives in Iraq and Afghanistan, commanders learned to organize their force to get casualties to medical care within sixty minutes or less – the "golden hour." Fighting the information fight will require similar model and a common mindset with the Joint Force.

Effective and timely response always requires unity of effort. Therefore, commanders must consolidate information related capabilities within their staffs consistent with the treatment that other Joint Functions receive. Piecemealed solutions cannot neither optimize a commander's intent nor win the information fight; doing so limits information operations and continues its current treatment as a boutique capability. This does not imply a need to consolidate operations at the highest level, but rather indicates that commanders at all levels require purpose-built sections to conduct the fight. Like conventional operations, the Commander must serve as the nexus for the information fight, particularly since victory without winning the information fight is almost impossible to achieve. Public Affairs, Information Operations, and Cyber all have a role to play in the domain, and we can only effectively integrate their respective functions through reorganization.

Lesson 4. Commanders must drive change. Senior leadership must be involved to transform the way the Joint Force addresses information warfare. Commanders must be agile and adaptive leaders willing to assume risk..

The impact of Gerasimov's leadership on Russian military transformation cannot be understated. Gerasimov used his position and influence to rebuild the Russian military, addressing capability gaps while leveraging new and innovative ways of fighting. Although Russian operations are the product of decades of study and experimentation on how the information revolution would influence the nature and conduct of war, it was Gerasimov who played a critical role in allowing the required changes to occur.

Transforming the U.S. military's understanding of

Continued on next page

Information as a Joint Function requires similar leadership. There will be risk and mistakes will be made, but lessons must be learned and implemented for the Joint Force to evolve. Countering adversary messaging may require changes in the gain-loss calculus used to protect sensitive capabilities; there is little sense retaining a strategic source, means, or method if it means losing the strategic fight. Most importantly, this effort must not sacrifice the values systems that make Western democracies possible and desirable. When mistakes occur, the Information domain must be used to accept responsibility for errors, not to obfuscate them. Effective information warfare for Western democracies requires a flawless perception of integrity. Decisions to limit or delay transparency and the conduct of deception operations must be used sparingly. Although using information to create a fog can be undeniably useful, the strategic impacts of misleading information consumers will rarely outweigh the benefits.

What next?

Persistent innovation ensures that our concepts of information warfare never stagnate; U.S. forces, and cyber and information warriors in particular, must never stop adapting to emerging technology and methodologies. Russia has learned this lesson, and we must pay attention and study their methods to inform our own operations. Not all game-changing innovations are original; we must selectively learn and study the Russian experience to inform and shape our own transformation. Information warfare, including cyberspace operations, requires encouraging innovative ideas within our own force, learning from the innovations of others, and empowering every member of the force to enact change. Information warriors must never forget that persistent innovation means investing in good ideas, regardless of their source.

---

1 Thomas, Timothy. "Russia's Information Warfare Strategy: Can the Nation Cope in Future Conflicts?" The Journal of Slavic Military Studies 27, no. 1 (2014): 101-2.

2 Thomas 2014, 102-4.

3 Joint Publication 1-0, Doctrine for the Armed Forces of the United States (2013): xii.

4 Blackburn, R. Alan. Joint Staff J7 Information Paper. (Washington, DC: Joint Staff, 12 July 2017).

5 Pynnoniemi, Katri. "Introduction." In Fog of Falsehood: Russian Strategy of Deception and Conflict in Ukraine, edited by Katri Pynnoniemi and Andras Racz, 13-19. Helsinki: The Finnish Institute of International Affairs, 2016, 18

6 Putin, Vladimir. "Russian National Security Strategy." Russian Federation. Moscow, December 31, 2015, Para 30.

7 Gressel, Gustav. Russia's Military Options in Ukraine. European Council on Foreign Relations. Berlin, April 27, 2016. http://www.ecfr.eu/article/commentary_russias_military_options_in_ukraine3010, 4-5.

8 Al Jazeera. "Timeline: Ukraine's Political Crisis." Al Jazeera Englise, September 20, 2014.

9 Al Jazeera, 2014.

10 Jonsson, O., and R. Seely. "Russian Full-Spectrum Conflict: An Appraisal after Ukraine." Journal of Slavic Military Studies 28, no. 1 (2015), 13.

11 See http://eng.syria.mil.ru/en/index/syria/reconciliation_bulletin.htm

12 Loveluck, Louisa, and Josie Ensor. "US Jets in Showdown with Russian Warplanes over Syria after Bombing of Pentagon-Backed Rebels." The Telegraph On-Line, June 20, 2016. http://www.telegraph.co.uk/news/2016/06/17/russian-warplanes-bomb-elite-british-backed-syrian-rebels/.

13 Russian Federation. Ministry of Defence of the Russian Federation Bulletin of the Russian Centre for Reconciliation of Opposing Sides in the Syrian Arab Republic (June 17, 2016). Moscow, Russia: Russian Federation, June 17, 2016. http://eng.syria.mil.ru/en/index/syria/reconciliation_centre_bulletins/more.htm?id=12087559@egNews.

Russian Federation. Ministry of Defence of the Russian Federation Bulletin of the Russian Centre for Reconciliation of Opposing Sides in the Syrian Arab Republic (June 18, 2016). Moscow, Russia: Ministry of Defense, June 18, 2016. http://eng.syria.mil.ru/en/index/syria/reconciliation_centre_bulletins/more.htm?id=12087693@egNews.

14 Syrian Observatory for Human Rights. "About 950 Children and Women between 2498 Citizens Killed by Russian Airstrikes during 9 Months." Coventry, United Kingdom, June 30, 2016. http://www.syriahr.com/en/2016/06/30/48087.

15 Syrian Observatory for Human Rights. "466 Civilians Including 200 Children and Women between 5415 Killed by Coalition Airstrikes." Coventry, United Kingdom, 2016. http://www.syriahr.com/en/2016/06/23/47962.

16 Shaheen, Kareem. "MSF Stops Sharing Syria Hospital Locations after 'Deliberate' Attacks." The Guardian Online. February 18, 2016. https://www.theguardian.com/world/2016/feb/18/msf-will-not-share-syria-gps-locations-after-deliberate-attacks.

17 Graham-Harrison, Emma. "Russian Airstrikes in Syria Killed 2, 000 Civilians in Six Months." The Guardian Online. March 15, 2016. https://www.theguardian.com/world/2016/mar/15/russian-airstrikes-in-syria-killed-2000-civilians-in-six-months.

18 Medvedev quoted in BBC. "Syria Conflict: Pressure Grows on Russia over Civilian Bomb Deaths." BBC Online. February 13, 2016. http://www.bbc.com/news/world-middle-east-35568692.

19 Moscow Times. "Russia Cuts State Spending on RT News Network." Moscow Times. October 11, http://www.themoscowtimes.com/business/article/russia-cuts-state-spending-on-rt-news-network/538390.html.

20 RT. "RT's 2016 Budget Announced, down from 2015, MSM Too Stumped to Spin?" RT (Russia Today). May 4, 2016. https://www.rt.com/op-edge/318181-rt-budget-down-msm/ Neu:

21 Chen, Adrian. "The Agency." The New York Times Magazine. New York, June 2, 2015. http://www.nytimes.com/2015/06/07/magazine/the-agency.html?_r=1.

782 MI Change of Command (cont.)

FORT GORDON, Ga. – *Lt. Col. Mathew Lennox (left), the outgoing commander of the 782nd MI Bn., accepts the battalion colors from Command Sgt. Maj. Christian Adkison, during his change of command ceremony at the Cyber Fitness Center on June 7. (U.S. Army Photos)*

Continued from page 8

as long as you take responsibility for your actions, learn from them, and are willing to stand up and teach other people so we don't make the same mistakes again in the future."

Lennox said the biggest lesson he learned from his command was "if you get to caring, committed and coachable, you've built a culture."

Thinking back, he believes it has only been in the last 180 days that the culture in his battalion really started to come out.

"There were little things the battalion did outside of work…people willing to get together outside of work, not levying work upon them outside of work, but just allowing them to get out and enjoy the company of one another outside of work," said Lennox. "About two weeks ago the lieutenants popped up out of nowhere, all wearing their Aloha shirts…I think they called it the 'Lieutenant Luau.' They are starting to form their own culture."

Proudest achievement

According to Lennox, building the NCO Corps is the one area he is most proud of.

"I just needed people to be 'caring, committed, and coachable' because I thought the one part we weren't was in taking care of Soldiers. And that all ties back to understanding the core of the team, understanding the value of the NCO Corps, and getting back to the basics, and taking care of Soldiers," said Lennox. "I think we've got a group of non-commissioned officers that really believe in taking care of their people, grooming their successors and propelling them forward to make the organization better."

What are you going to miss?

"The people. There's some real talent in this battalion," said Lennox. "I think we generated a whole new level of buy in from the Civilians in this battalion, in terms of just letting them do their jobs."

He mentioned Army Civilians like West Lewis, Connie Hamilton, and Cece Shoffner, and "there's a whole host of other people. We have had some first-class people in this battalion," said Lennox.

"We have managed to grow. In fact, we probably had the lowest civilian attrition rate this battalion has ever had. We have retained talent such as developers and Civilian operators – people who could go out and make more money elsewhere, but have found something in the job here, and made the decision to stay with us. That commitment has been awesome and it has truly been an enabler for the teams."

The fourth commander of the 782nd MI Battalion (Cyber) – Cyber Legion! Silent Victory!

"Dave Chang handed over a solid organization, and we have grown a lot," said Lennox. "I believe Wayne Sanders is going to take over a battalion that is firing on all cylinders, but that's not enough. Just like when I came in, wherever we are at today, we are not going to be asked to do less. He's going to have to find the resources and the leaders to do more."

However, Lennox believes Sanders is "absolutely the right person to do it. He's been in the brigade,

FORT GORDON, Ga. – *Lt. Col. Wayne Sanders, commander of the 782nd MI Bn., makes his remarks to the Soldiers, Civilian, Family members and friends of the 780th MI Bde., during his change of command ceremony.*

he's done the S3 (operations) job, the XO (executive officer) job, and the team lead, so in many ways he's more familiar with the organization than even I was when I got down here."

Lt. Col. Sanders' most recent assignments include serving as the chief of Cyberspace Electromagnetic Activities (CEMA) Support to Corps and Below (CSCB), U.S. Army Cyber Command, as the team lead for 23 National Mission Team, Cyber National Mission Force, U.S. Cyber Command (USCYBERCOM).

In his comments to battalion Soldiers and Civilians, Vile remarked, "Fifteen years and over six thousand miles away in a place called Mosul, your new commander stood out even in a Brigade of exceptional Soldiers. Along with a young warrant officer named Al Mollenkopf (currently the Command Chief Warrant Officer at USCYBERCOM), Wayne and his team fundamentally changed the way that SIGINT (Signals Intelligence) drove operations. His innovation, coupled with an agile, adaptive, and opportunistic force, created operations successes beyond anyone's expectations."

Over the next 12 months the Lennox Family will be in Carlisle, Pennsylvania, where Lt. Col. Lennox will attend the Army War College. He is already anticipating his follow-on assignment – coming back to the cyber Family and taking command of the 780th MI Brigade (Cyber) where he will continue his philosophy of creating a culture of "caring, committed, and coachable" soldiers and civilians.

Praetorians -- Strength and Honor

Immortals (cont.)

Continued from page 16

analysts and other supporting military occupational specialties Soldiers, which gave Soldiers and Army Civilians technical training they may not have had a chance to experience otherwise. It also provided B Co's leadership a chance to identify potential talent.

After the exercise, most of those involved left feeling like the training was a worthwhile event.

"Bravo Company's Attack and Defend exercise had all the qualities of a professionally designed, well organized, real-world training exercise," said Staff Sgt. Gregory Waxmonsky. "In three and a half years working in the cyber operations field, I haven't had a training exercise that comprehensive since my JCAC capstone exercise. And while there are always ways to improve, I would definitely want to do something like that again!"

"The (Attack and Defend) exercise exceeded my expectations," added Spc. Rudolph Esterberg. "Granted, there was a lot of room for improvement, but the overall layout of this exercise and the direction it was going have great potential to be a very practical and educational simulation of both offensive and defensive cyber operations."

As the first iteration of B Co's Attack and Defend exercise, a few bumps in the road were expected. However, Capt. Master and his team received great feedback from those involved on how to improve as they prepare to unveil an upgraded iteration of the exercise at AvengerCon this fall.

FORT GEORGE G. MEADE, Md. – *Capt. Lauren Feifer, the commander of the B Company, 781st Military Intelligence Battalion (Cyber), salutes at the completion of her change of command ceremony at the McGill Training Center, August 5.*

A Nibble on Innovation (cont.)

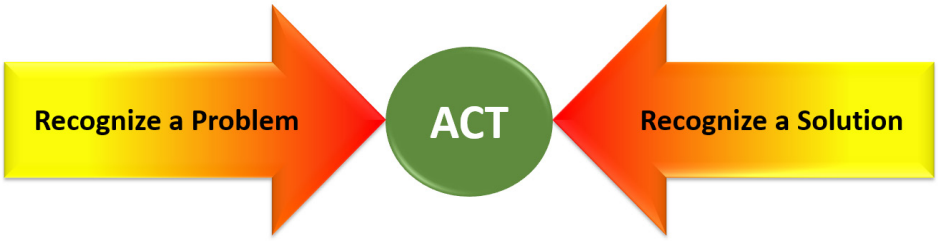


Figure 3: The key to innovation is Action

Continued from page 6

As I researched how to become more innovative, I read that it may be best to think in problems vice solutions. There is conflicting commentary on whether you should conduct problem-oriented or solution-oriented thinking. I think there is room for both with the goal being an implementable solution. However, for those who struggle with innovation, identifying problems first may serve as a catalyst to generate solution-oriented thought. Another advantage of problem-oriented thought is that a solution that doesn't solve a problem will generally wither on the vine as it will lack relevance (https://medium.com/swlh/start-with-problems-not-solutions-8521c53264b2).

Action is initiative in motion. Oftentimes, initiative is governed by time, energy, and the amount of support offered to the individual by peers, management, and leadership. If these are out of balance, initiative may be stifled and personnel may not act as readily as necessary to solve problems in new and innovative ways. It takes a certain amount of fortitude to act on a problem as there is a bit of risk involved. The outcome may result in failure, policy may not be designed to support a particular activity, leadership may not grasp the value in a project, etc. However, be courageous and act – you may find success where others have not.

The CMF has some of the most talented personnel in the Army. Generally, time and energy are the primary limiting factors in accomplishing a given task rather than a lack of technical expertise. Innovation is a time, energy, and resource intensive activity that the operational force needs to budget for at the individual level. This requires the organization to not only encourage innovation, but to allot time and resources for personnel to experiment and research various technologies, techniques, and processes that will improve the mission. I need your help to figure out the best means to facilitate this in an expedient and achievable method.

Persistence is often a winning strategy when it comes to innovative discovery and solution implementation. Anyone who has been in Cyber, Intelligence, and Signal know the many challenges across policy, political, and timing boundaries that arise when attempting to implement something new into the system. The best advice I have is to exhibit patience, be persistent, and continue to push forward – If you're not, then it's likely that no one else is.

Solutions can be the result of purposeful intent; however, they may also be the result of happenstance – or accident, if you will. There are numerous examples throughout history that highlight this; plastic, microwave oven, x-rays, penicillin, etc. That said, the people who discovered these innovations by were highly prepared to recognize the solution and implement it when the opportunity arose. Prepare yourself technically, professionally, and tactically to identify and meet challenges as they arise. This is hard, demanding work, but the outcome on a personal and professional level are well worth the effort.

I look forward to seeing what innovative solutions that our team comes up with in the future. Remember, innovation is not limited to a select few. Anyone can participate, all it takes is preparation, the fortitude to act, and persistence.

Vanguard 6 (cont.)

Continued from page 4

Let us know how we're doing!

Changes are happening, and more are coming up. If you're planning to start an AIP action soon, make sure you have the latest templates and GEARS routing. As your packet is processed, assess how we could further improve the process. Despite AIP being one of many routine battalion processes, I have directed that AIP packets will have priority.

This is my program. 1st Sgt. Stanley Collins and I are absolutely committed to optimizing the performance of AIP processing. My door is always open. WE GOT THIS!!

"Vanguard...When Others Cannot!"

ARLINGTON, Va. *– Soldiers and Civilians representing the Headquarters and Headquarters Company, 780th Military Intelligence Brigade (Cyber), took part in a Wreath Laying Ceremony at the Tomb of the Unknown Soldier at Arlington National Cemetery on July 4. (U.S. Army Photos)*

For Teens

HACKATHON

Advance through computer game levels to hone your hacking skills!
Registration is required.
Limit 20 participants.

Tuesdays, September 10, October 8, November 12 from 4:00-7:30 PM

Presented in partnership with the
780th Military Intelligence Brigade (Cyber)

ODENTON REGIONAL LIBRARY

Anne Arundel County Public Library
Educate. Enrich. Inspire

ODENTON, Md. *– The Soldiers and Army Civilians of the Headquarters and Headquarters Company, 780th Military Intelligence (MI) Brigade (Cyber), and 781st MI Battalion (Cyber) will partner with the Anne Arundel County Public Library (AACPL) to host a STEM event on three separate dates this fall from 4 to 7:30 p.m. at the Odenton Regional Library. Participation is limited and teens only need to have an AACPL account. To register, go to the AACPL website at: https://www.aacpl.net, or visit the Odenton Library at 1325 Annapolis Rd.*

Carbon Monoxide (cont.)

Continued from page 30

- Take a head count.
- Do not reenter the premises until emergency responders have given you permission to do so.

The CDS offer additional tips:

- Have your furnace, water heater and other gas burning or coal-burning appliances serviced by a qualified technician every year.
- Do not use portable flameless chemical heaters indoors.
- Have your chimney and cleaned every year, and make sure your fireplace damper is open before lighting a fire and well after the fire is extinguished.
- Never use a gas oven for heating your home.
- Never use a generator inside your home, basement or garage or less than 20 feet from any window, door or vent; fatal levels of carbon monoxide can be produced in just minutes, even if doors and windows are open.
- Never run a car in a garage that is attached to a house, even with the garage door open; always open the door to a detached garage to let in fresh air when you run a car inside.
- If you drive a car or SUV with a tailgate, when you open the tailgate open the vents or windows to make sure air is moving through. If only the tailgate is open CO from the exhaust will be pulled into the car or SUV.

Stay safe!

CyberCamp (cont.)

Continued from page 36

'no, this was my place of duty.' I think, going forward when other Soldiers and Civilians see this they might volunteer as well."

Wissmann said the other CyberPatriot volunteer, who has worked behind the scenes, is Regina Giles. He said that Giles was the strategist who was the driving force behind getting the CyberPatriot program established at Meade High, as well as another high school in Chantilly, Virginia.

Serota is very thankful for the CyberPatriot mentors who have volunteered in their personal time to instruct and mentor the students throughout the school year and CyberCamp.

"The mentors are professionals with expertise that we don't have in the school system. We have a lot of dedicated educators, but very few, if any that have that professional, hands-on experience."

Serota said that Anne Arundel County Public Schools interested in starting their own CyberPatriot program should contact AFA, have an educator willing to accept the additional responsibility, and a computer lab. If the school doesn't have the expertise, they could request mentors, either by contacting the Fort Meade public affairs office or one of the many cybersecurity companies within the central Maryland area. AFA provides all the training materials, the student and facilitator guides, the specs, and the virtual machine images for the competitions.

FORT GEORGE G. MEADE, Md. *- The students and mentors for the CyberPatriot CyberCamp 2019 at Meade High School, July 29. (U.S. Army Photo)*

Sgt. Kyle Tamraz, B. Co., 781st MI Bn. Q & A

FORT GEORGE G. MEADE, Md. *- Congratulations to Sgt. Kyle Tamraz, B Company, 781st Military Intelligence (MI) Battalion (Cyber), 780th MI Brigade (Cyber) for winning INSCOM's Best Warrior Competition. VANGUARD! (Photos by Bill Roche, ARCYBER Public Affairs)*

Q. If someone asked you why you're competing what would you say to them?

I would tell them that I am competing to better myself and to represent the unit the best that I can.

Q. Would you recommend the competition to your peers, and if yes, why?

Absolutely, I would recommend the competition to my peers. It is a great way to get your name known within the unit and the further you go the more people get to see who you are.

3. What was the toughest part of the INSCOM BWC and what are you going to focus on for the next level?

The toughest part of the competition was the board. I did not have much time to prepare for it and never received the MOI so, that was challenging. I plan on having plenty of mock boards and studying vigorously for the ARCYBER board.

4. Anyone you want to thank or want to add?

I want to thank my battle buddies Matthew Bryant-Rojas, Deonte King, and Noah Heintze for supporting me and helping me prep for the competitions on their own time. Also, would like to thank my girlfriend, Cayla Dempsey, for her continued support for the competitions and always encouraging me to give it my all. Lastly, I would like to thank Sgt. 1st Class Herrera for always going out of his to help prep me in any way that he can to help me better myself.

AvengerCon IV

October 17th & 18th, 2019

Register now at:

https://www.avengercon.com/index.html

AVENGERCON

EVERYWHERE AND ALWAYS...