780th MILITARY INTELLIGENCE BRIGADE (CYBER)

THE BYTE

Vol. 10, Issue 3

WARRANT OFFICERS
Past, Present, and Future

Quiet Professionals

By CW4 Erin Ward, Senior Technical Advisor, 780th Military Intelligence Brigade (Cyber)

OFTEN REFERRED TO AS THE "QUIET PROFESSIONALS," each Warrant within our current formation contributes unique skills and subject matter expertise, helping to drive the team — and the mission — forward. In this edition of The BYTE magazine, we will feature perspectives and insights from across the Brigade's Warrant Officer Corps, including Cyber, Signal, Military Intelligence, and Field Artillery, as well as insights from outside organizations. Our hope is to illuminate their significant contributions and how they are working deliberately today to help us shape the capabilities of tomorrow.

I have spent my past five years in many roles throughout the 780th Military Intelligence Brigade (BDE), having served on teams in both Battalions, the BDE Headquarters & Headquarters Company at Joint Mission Operations Center-Maryland, and now as the BDE Senior Technical Advisor (STA). As the BDE STA over the past year, I have had one main goal, to ensure the success and evolution of the Warrant Officers in this formation.

As I work with this team, I found myself surrounded by an amazing cohort of people who solved complex problems, mentored those around them, and did jobs they weren't asked to do. These are not the rumored Warrants leaving their hats at the desk and leaving for the day. These are reliable leaders you need when the going gets tough.

Warrants are the groups of people solving the problems you didn't know you had and doing the work, more often than not, as the quiet professionals I mentioned previously. We provide the technical depth needed to solve multifaceted problems and the leadership required to drive project operations. Both expertise and leadership in this capacity are hard to define in concrete terms – but you know them when you see them. In this issue, we will illuminate some of the precise challenges they are tackling and introducing you to the expertise they provide. Specifically, within the Cyber branch, we have 170As, 170Bs, and 170Ds in the BDE serving as all variations of operators, exploitation analysts, and developers. The 131As are vital to the mission, bringing their distinct skill set in targeting, guaranteeing mission success. The 352Ns are the subject matter experts in military intelligence domain bringing the necessary knowledge to the teams. The 255As, 255Ns, and 255Ss are integrated across the BDE teams enabling in areas such as malware analysis and infrastructure support. These Warrants also work as trainers, adjunct faculty, exercise assessors, curators for work roles, PCTE (Persistent Cyber Training Environment) experts, and mentors across the BDE, in addition to their jobs on the teams.

Warrant Officers are a powerful network of technical professionals. During my enlisted time in 4/2 Stryker BDE out of Joint Base Lewis McChord, CW3 Steven Robinson took me under his wing and showed me what it was like to be "part of the mafia." I saw firsthand the power of the Warrant Officer network. At any time, he could pick up the phone and call another Warrant for help, and they would be there. I guarantee if you ask any Warrant, they remember the Warrant Officer that made them want to join this network. That is what makes being a Warrant Officer so special – the decentralized way we can navigate our network to find the right person with the right skill set to solve our current problem.

Building on this powerful network, Warrant Officers recommend and recruit our own replacements. The Warrant Officers in our formations today are there because someone identified an NCO with exceptional abilities, technical depth, and growth potential who could accomplish more with those skills and abilities. Paraphrasing something Mr. Scott Brown from the 780th BDE S3 shop said in passing, "If you look at a Warrant Officer straight on, you see the technical expert; if you take a step to the side, you see a network of Warrant Officers." He was spot on. I also believe when you step to the side you see the lineage of Warrants that came before them making this cohort what it is today. Warrant Officers are continuously seeking to develop and mentor the next generation. I encourage any Soldiers who are considering the Warrant path to take the first steps toward becoming Warrant Officers.

Finally, I would be remiss if I did not pause to appreciate all who supported me on my journey. I have been surrounded by an amazing team of Officers, Warrant Officers, NCOs, Soldiers, and Civilians who helped ensure my success as an NCO and helped make me the Warrant I am today. I also take what I learned as an NCO and use it daily as a Warrant Officer. I am still surrounded by a network of Warrant Officers who continue to mentor me, just as it is my responsibility to mentor other Warrant Officers. We are inevitably tethered together from our past, in our present, and into our future based on the fundamentals of being a Warrant Officer.

Looking around the organization today, given our current operational pace, there is no indication of us slowing down. As we look to the future, we will need to continue to orient, evaluate and act against complex challenges. I have no doubt the Warrants in our formation will rise to the challenge of being the professionals we need to outpace our adversaries and to continue to grow our Warrant Officer cohort into the future. ■

PRAETORIANS

SENIOR TECHNICAL ADVISOR

780th MI BDE
"STRENGTH AND HONOR"

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

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

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

All photographs published in The BYTE were taken by 780th MI BDE Soldiers, Army Civilians, or their Family members, unless otherwise stated.

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

On the Cover

U.S. Cyber Command team member work in the Integrated Cyber Center, Joint Operations Center at Fort George G. Meade, Md.

The Clock is Ticking

The clock is ticking. I did not hear it for the first 21 months in command. I hear it now.

Leaving the brigade looms large. I have spent time in the 781st, commanded the 782d, and finally led "those people at brigade." My time here feels incomplete. We achieved most of my goals. Others eluded me. I learned stuff, and I am still confused by things. Frankly, I am unsure if the motto is "Strength and Honor" or "Everywhere and always in the fight." One slogan is on my office wall; the other is on the front of the headquarters. (I use "Everywhere and always in the fight" 61 percent of the time.)

I am passionate about the 782D motto: "Silent Victory!" It simultaneously means nothing and everything. It means nothing to the skeptic. A skeptic might ask: "What has cyber ever won?" or "What about this issue?"

The first question is misguided. "Silent Victory" means everything if you know what our teams can do, what the developers can produce, how much the special staff cares, and how our Guardsmen innovate. It means everything if you have been around the more than 1800 Soldiers and Civilians in the brigade.

The second question misses the point; most issues are simply misunderstandings. Misunderstandings can compound and become emotional for those involved. To address misconceptions, we need to be patient and work together. We need to be more resilient, tolerant, and open to seeing the other side. We need to speak up and get down to resolving adversity at the lowest level.

Overcoming adversity is the key to winning. That is true if you have problems during a mission, challenges in the office, or watch Marvel movies. As I walk around the brigade, I often ask, "Are we winning?" Most of the time, I hear a resounding yes. Sometimes I hear, "at what?" One day, Scott Brown and Doc Eden replied that we are all winners.

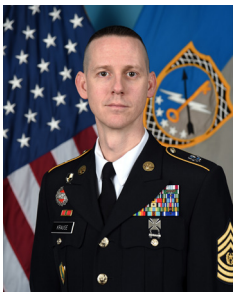
I did not realize it at the time, but there was absolute truth in their statement. The brigade is full of winners. People throughout this organization produce victories every day. It is truly remarkable.

It has truly been an honor to serve in this brigade and with our people. As I depart the brigade, I would ask that you take the time to celebrate what makes this organization great. Celebrate the people. Celebrate the silent victories. ■

Respectfully,

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

Be Brief, Be Brilliant, Be Gone



"Be brief, be brilliant, be gone…" so quoted a warrant officer when talking to a group of us (I was still a young private at that time); he then proceeded to say "I, will be at least two of these!"

This knowledgeable and humorous warrant officer was one of my early introductions to this amazing cohort of technical leaders. I truly would not be who I am, or where I am today without the mentorship, guidance, and support of so many great warrants. I would say that I probably disappointed several as they worked very hard for me to submit my packet and join their illustrious ranks. Unfortunately, it was not meant to be, yet I appreciate every single warrant officer's commitment and thoughts. They are the sounding boards and innovative drivers that we need to move us into the future.

Aside from my personal appreciation of warrant officers, I wanted to share two quick thoughts that I would like you to keep in mind while reading the rest of the articles and in your daily interactions with the force.

First, warrant officers are the professionals and leaders who are charged with overseeing the technical health and direction of Soldiers, Capabilities, and Operations.

Second, the future of the force and how we evolve is conceptualized, developed, and implemented through the technical acumen and drive of our warrant officers.

We, as an Army, are more successful because of their experience, continued learning, professional growth, and leadership. From their investment in others as well as themselves, it is this dedication that enhances the Army's technical skills and capabilities. These true technical leaders ensure our training and tools meet operational requirements, while keeping an eye to the future.

Thanks specifically to: Tim McGinty, Wendy Wayman, Mark Attanasio, Donna Dixon, Earl Kimmerly, Bliss Payne, Mike Ach, Mark Mollenkopf, Travis Ysen, John O'Reilly, and Erin Ward. I would not be as successful, nor would this Army be as great without all of you, your families, and your sacrifice. Thank You! ■

Respectfully,

Ronald Krause
CSM, USA
Command Sergeant Major, 780th MI BDE (Cyber)

[1]. President Woodrow Wilson

Vanguard Support to the Cyber National Mission Force

By CW3 J. Paul "JP" Dixon, Senior Technical Advisor, 781st MI Battalion (Cyber), USCYBERCOM Mission Director

ON ITS SURFACE, THE MISSION OF THE 781ST MILITARY INTELLIGENCE BATTALION is like many other units that support an operational command. Like other units, you will often hear the mantra of "man, train, and equip" in battalion and brigade staff meetings, update and training briefs, and unit status reports as major efforts and milestones are discussed. Like other Army battalions, you will also find Warrant Officers lending their expertise and experience to those efforts as they establish processes, and both create and refine standard operating procedures (SOPs). When you dig a little deeper, you will find that the 781st and its Warrant Officers go well beyond the "man, train, and equip standard. To understand just how much, and what, Warrants do in 781st, you need to understand who and what they support.

The 781st supports the United States Cyber Command (USCYBERCOM), Cyber National Mission Force (CNMF). CNMF plans, directs and synchronizes full-spectrum cyberspace operations to deter, disrupt and if necessary, defeat adversary cyber actors to defend the U.S.1 Unlike the Cyber Combat Mission Force (CCMF), which is composed of service provided Cyber Protection Teams (CPTs), Combat Mission Teams (CMTs), and Combat Support Teams (CSTs) which are operationally controlled by Joint Force Headquarters – Cyber (JFHQ-Cs) and aligned to geographic Combatant Command (CCMD) requirements, CNMF effectively acts as the action arm for the Commander of USCYBERCOM. This complex, global mission encompasses both offensive and defensive actions in and through cyberspace that are tied to preventing state sponsored and foreign criminal cyber actors from threatening or harming the United States. Whether it is preventing ransomware attacks against critical infrastructure, responding to foreign influence operations and attempts to undermine elections, or exposing Malicious Cyber Actors (MCAs) and their tools; chances are that a 781st Warrant Officer was involved in making it happen. There is a lot behind those words, "man, train, and equip".

Man

First and probably foremost, the 781st provides the Soldiers that fill out approximately 350 positions in the CNMF. Of that, there are more than 50 Warrant Officer billets for critical positions as Cyber Capability Developers (MOS 170D), Fires Planners (MOS 131A), Signals Intelligence Technicians (MOS 352N), Cyber Defense Analysts (MOS 255S), and the Cyber Operators, Exploitation Analysts, and Cyber Planner roles filled by Cyber Warfare Technicians (MOS 170A).

Those are the Warrants who advise the CNMF Commander, Task Force Commanders, and senior officers and Civilian leaders as well as mentoring and training Soldiers, Sailors, Airmen, and Marines. They are often the innovators and problem solvers who draw on that combination of technical expertise and knowledge, knowledge of doctrinal process and procedure, and most importantly operational experience to lead our teams to success. Those Warrants are often called upon to develop and refine guidance and policy, SOPs, and to support staff functions.

Warrant Officers have filled positions as the Master Fires Planners leading CNMF targeting processes, Weapons and Tactics Directors responsible for operational oversight and risk management, Task Force Mission Directors synchronizing operational lines of effort, Senior Intelligence Analysts and Reporters leading Analysis and Production teams, as Cyber Planners driving and coordinating offensive and defensive activities, and as the operators directly engaging the enemy. All that said, it's not enough to just provide talent. The 781st is also responsible for training those Soldiers.

Train

While making sure CNMF has the forces it needs, the 781st also plays a crucial role in training the Soldiers who serve there. As one would expect, Warrants serve as trainers and mentors within the operational force. Not only do they teach their team members, but they also identify training gaps, develop training, and share that knowledge to strengthen the force as a whole and assist the Army Cyber Center of Excellence in their mission. Specific examples include developing Cyber Operator and Exploitation Analyst training ranges and the Mission Commander Course. As experts in their craft, 781st Warrants serve as work role curators responsible for reviewing and establishing requirements and certification standards for their respective specialties.

Training also encompasses a responsibility for ensuring the force is trained to standard. To that end, the Warrants of the 781st also serve as assessors who evaluate the teams and Task Forces and their ability to perform all their required tasks and functions. In fact, Warrants have played critical roles in developing the Collective Training Exercise (CTE) scenarios, the technical ranges, and implementing and executing the first CNMF CTEs which certified two Task Forces.

Equip

Equipping the CNMF is far different

from equipping traditional Army maneuver units. The "weapons" used in cyber warfare are often computers, networks, and the ever changing and ephemeral capabilities, tools, tactics, and techniques that are used in the execution of the cyber mission. These kinds of "equipping" challenges demand rapid and innovative solutions, well-defined requirements, and sometimes hands-on development. As with other mission areas, 781st Warrants are almost always in the middle of the equipping efforts.

Cyber Capability Development is one of the most important and technical functions that Warrants support. While the Officers and enlisted Soldiers of the 781st possess incredible intellect and talent as software developers, it is often the Warrants who bring the practical experience of employing capabilities and working within DoD processes to the effort. As with other areas, they are also deeply involved with establishing the qualification requirements and standards for developers within the force. They also are often called upon to inform the development, construction, and acquisition of hardware solutions to solve other problems.

In the fast-paced mission that CNMF is responsible for, the mission requirements can easily outpace what you are actually equipped for. In those cases, it has often fallen to Warrants to ply their knowledge of the technical aspects of the problem, the resource and acquisition processes, and policy requirements to quickly identify and sometimes create solutions. Whether it was getting the right equipment to support deploying a Cyber Protection Team on a Hunt Forward Operation or helping to establish secure and reliable communications for dispersed forces, 781st Warrants have been a part of creating the solution.

Future

What the future holds for the Battalion is yet to be written. We already know that USCYBERCOM and CNMF will continue to grow, just as the nation realizes the size and gravity of the problem of defending U.S. interests in cyberspace. It seems likely that the 781st MI Battalion (Cyber) will be called on to grow and meet those challenges too. To ensure that the battalion and the Army has the Warrants it needs, we must start preparing now.

With all the demands that fall on the battalion and the increasing tempo of CNMF operations, the demands on and for talented Warrant Officers continue to increase. The responsibility for filling that demand ultimately falls back on the current Warrant Officers. It is incumbent on us to teach and mentor Soldiers, to identify those who have the ambition and talent to become Warrant Officers, to guide them in their careers, and to recruit them into our ranks. ■

References:

[1] "Cyber Command task force focuses on emerging threats". C4ISRNET. March 8, 2021. https://www.c4isrnet.com/cyber/2021/03/08/cyber-command-task-force-focuses-on-emerging-threats/

[2] "Cyber 9-Line" Improves Cybersecurity and Enables Election Integrity". U.S. Cyber Command. June 9, 2020. https://www.cybercom.mil/Media/News/Article/2213264/cyber-9-line-improves-cybersecurity-and-enables-election-integrity/

[3] "New CNMF initiative shares malware samples with cybersecurity industry". U.S. Cyber Command. November 5, 2018. https://www.cybercom.mil/Media/News/Article/1681533/new-cnmf-initiative-shares-malware-samples-with-cybersecurity-industry/

[4] "Cyber Command has deployed to nations 27 times to help partners improve cybersecurity". Fedscoop. March 4, 2022. https://www.fedscoop.com/cyber-command-has-deployed-to-nations-27-times-to-help-partners-improve-cybersecurity/

State of the 782d Military Intelligence Battalion (Cyber)

By CW4 Laurie Sammons, Senior Technical Advisor, 782d MI Battalion (Cyber)

THE 782D MILITARY INTELLIGENCE BATTALION, headquartered at Fort Gordon, Georgia, is the largest battalion within the 780th Military Intelligence Brigade (Cyber). The battalion mans, trains and equips operational Combat Mission Teams (CMT) and Combat Support Teams (CST) spread across four locations: Georgia, Maryland, Texas, and Hawaii. These teams are responsible for providing offensive cyberspace operations in support of U.S. Cyber Command and multiple Geographic Combatant Command (CCMD) priority strategic objectives. At the heart of these operations are the Warrant Officers. The Warrant Officers in the Battalion (352N, 131A, 170A & 170D) fill key critical roles in support of our Soldiers, Civilians, and their families. With a focus on the Battalion's three primary goals (people, mission, and balance), our Warrant Officers are the lead for team validation and mission readiness, operational planning team leadership, Project Management, and infrastructure control, all while maintaining their own technical and tactical professionalism and readiness.

People are the first primary goal since our personnel are the key to the Battalion's success. Our Soldiers and Civilians help us meet our daily requirements and objectives, so taking care of them and their families by providing a better quality of life at work is our focus. Effective engagements with Ft. Gordon leadership to improve the barracks for our single Soldiers, leadership battlefield circulations (BFC), and participation in battalion, garrison, and brigade level events are examples of just a few areas in which our Warrant Officers are currently involved. As Warrant Officers in the Battalion, we facilitate some of those engagements and continue to strive and recruit the best and brightest within our ranks. Warrant Officers helped lead many efforts in the Battalion by recognizing the talent, providing mentorship sessions, leading training events, and actively participating in Company, Battalion, Brigade, and Army Cyber events. For example, WO1 Weeks led a team of Soldiers that successfully won first place in the Joint Force Headquarters-Cyber (JFHQ-C) Army analyst competition among all teams assigned to Army Cyber (ARCYBER).

The team's mission is an important and essential goal to meet the Battalion's operational requirements. Our teams are spread across four different states supporting all JFHQ-C components (Army, Navy, Air Force, and Marines) and the CCMD's mission objectives. Many of the Warrant Officers are selected to fill additional duties within the JFHQ-C as subject matter experts to lead offensive cyberspace operations. Field Artillery, Military Intelligence, and Cyber Warrant Officers work together to lead daily operations, collaborate with external agencies, and translate strategic objectives into operational and tactical objectives to support the CCMD's end state.

Balance is the third, but equally important component to the goals of the Battalion. As leaders it is our responsibility to help our personnel find a balance between operational, administrative, personal, and family requirements. It is a key factor to be an effective organization while encouraging personnel to rotate among teams to learn new skills and decompress. When stress becomes a destraction, leaders both encourage personnel to seek help or provide them a crucial sounding board. We have a great chaplain and Military Family Life Counselor (MFLC), they are both very engaged and always available to our personnel. It is the most important goal we share as leaders in the Battalion.

The Battalion continues to grow in mission and size with the development of four new teams by the end of 2024. The growth will bring new challenges, personnel, and capabilities. As leaders we need to be agile, innovative, and develop ways to share information, knowledge, and training. It will allow us to meet requirements, expectations and be ready to support current and future operations. The Warrant Officers in the Battalion are ready for the challenge ahead and continue to synchronize activities to support Battalion and Brigade leadership. As a Battalion, we are working together to achieve JFHQ-C commanders' objectives while conducting full spectrum, multi-domain, offensive cyberspace operations. ■

915th Cyber Warfare Battalion on the Rise

By CW4 Ryan Rappold, Senior Technical Advisor, 915th Cyber Warfare Battalion

UPON RECEIVING ORDERS TO THE 915TH CYBER WARFARE BATTALION (CWB) earlier this year a barrage of opinions and questions were hurled at me from many directions about what the 915th CWB foundationally is and is not. The surprising element to most of the engagements was the lack of understanding and consensus from outside the organization on what the perceived 915th CWB's mission and vision for the future is. What I discovered in my short time on ground is that the leaders and Soldiers of the 915th have been diligently working to manifest the unit's first deployable Expeditionary Cyber Electromagnetic Activities (CEMA) Teams (ECT), investigating, and acquiring capabilities, and attempting to birth innovative concepts and strategies of employment while confronting the challenges of contributing to the understanding and shaping of nascent doctrine defining the units' operations. The labors of these Soldiers to originate the unit are reminiscent of the founding of the U.S. Army Cyber Protection Brigade (USACPB) and the 780th Military Intelligence Brigade while developing Cyber Protection Teams and Combat Mission Teams. Current 915th efforts are like USACPB and 780th early efforts to build, train, and conduct missions all the while learning, adjusting, strengthening, and improving. The purpose of this article is to provide information on the 915th to increase general understanding of its mission and contribute to the way forward discussion for the organization.

The 915th CWB was originally established as a Table of Distribution and Allowances (TDA) organization. The organization is in the process of transitioning to the 11th Cyber Battalion and will become a Table of Organization & Equipment (TOE) unit. The 915th CWB was established with a mission to conduct information warfare (IW) in the cyber domain and electromagnetic spectrum (EMS) by employing Offensive Cyberspace Operations (OCO), Defensive Cyberspace Operations (DCO), Electronic Warfare (EW), capability development, and Information Operations (IO). The CWB provides deployable ECTs to enable delivery of capabilities at operational and tactical echelons across the competition continuum for Large Scale Combat Operations (LSCO) during Multi-Domain Operations (MDO). In addition to MDO, the 915th CWB mission emphasizes providing tactical-level CEMA Support to Corps and Below (CSCB) throughout periods of competition and conflict. An examination of 915th CWB's tasks and goals, as well as the unit's characteristics that makes it unique, helps to inform the unit's way ahead. As the CWB continues to build capabilities, increases capacity from three ECTs to twelve, and refines CEMA tactics, techniques, and procedures (TTP) the organization will tirelessly work to strengthen supported Command Relationships (COMREL), work with supported units to improve comprehension and integration of IW capabilities by helping to define requirements, and refine interaction and authorities processes with Joint Forces Headquarters – Cyber (JFHQ-C), U.S. Cyber Command (USCC), and Army Cyber Command (ARCYBER).

Enumerating tasks and goals helps establish a framework for the unit as it continues to build additional teams and increase capabilities. It is important to understand unit deliverables to ensure training, authorities, capability acquisition, and development align with objectives. For the purposes of this article, an introduction to a few of the unit's tasks helps establish a framework for discussing strategies for moving the organization forward. Among the unit's goals are providing cyber and EW support to land maneuver and enabling freedom of maneuver in cyberspace. Tasks that assist in achieving those goals include detecting and identifying signals of interest in the EMS, identifying and exploiting vulnerabilities in adversary critical systems, developing and deploying capabilities in support of OCO and EW efforts, providing proximal EW and OCO access and targeting, defeating adversary long range anti-access area denial (A2AD) systems, neutralizing adversary A2AD mid-range systems, providing reach-back support capabilities, and conducting military information support operations through tactical deception, specialized content creation and delivery.

In addition to enumerating tasks, identifying the capabilities that make the unit unique adds to the requisite organizational understanding necessary for charting a way ahead. The 915th's expeditionary nature combined with its promise to deliver OCO capabilities forward and its emphasis on CSCB and support to MDO distinguishes the unit's mission among Army cyber. The ability to employ forward forces and enable proximal access in support of cyber and EW operations for the CSCB and MDO missions, as well as for other communities of interest, is a unique capability for the unit among conventional forces. This expeditionary capability allows the unit to offer unique enabling services for the joint force such as creating last mile establishment opportunities in contested and denied remote terrain. The unit can also provide commanders local resources for cyber-enabled surveillance and reconnaissance, when operating under the appropriate authorities. The 915th provides local resources to assist commanders in defeating adversary IW capabilities and its IO mission provides resident capability to disrupt adversary decision making by interjecting doubt in their observe, orientate, decide, act (OODA) loop.

The re-emergence of great power competition and the 915th's mission to provide capabilities in support of LSCO

during MDO presents the unit with exciting and hard challenges. Adversaries like Russia and China have been diligently working to develop, test, and employ A2AD capabilities intended to keep U.S. forces at more than an arm's length away as they attempt to accomplish regional strategic objectives both below the threshold of armed conflict and, in Russia's case, with the use of traditional military force. The premise of A2AD capabilities and systems is to deny entry into a contested area (TRADOC PAM 525-3-1, 2018, p. 7). Employment of this strategy seeks to create A2AD systems layers that includes Electronic Warfare, counterspace, offensive cyber capabilities, and advanced long range strike capabilities. These tactics are intended to destroy space-based reconnaissance and communications platforms crippling command and control and Intelligence, Surveillance, and Reconnaissance efforts, while also targeting military support operations (TRADOC PAM 525-3-1, 2018, pp. 11-12). These tactics are anticipated to significantly challenge U.S. global freedom of maneuver, navigation, and deployment in preparation for and execution of combat operations. Potential global adversaries have been studying U.S. tactics over the last two decades of operations in Iraq, Afghanistan, Syria, Yemen, and Africa gleaning important lessons resulting in development of A2AD strategies (TRADOC PAM 525-3-1, 2018, p. i).

The U.S. development of MDO seeks to find a way to "neutralize" and "defeat" potential adversary A2AD capabilities through the compete, penetrate, dis-integrate, exploit, and re-compete Strategy. This strategy attempts to discover windows of opportunity to penetrate adversary A2AD capabilities for exploitation at a time and place of maximum advantage in conflict (TRADOC PAM 525-3-1, 2018, p. v). The 915th has a role in the MDO battle, in partnership with Multi-Domain Task Forces (MDTF) and Combatant Commands, to investigate and target A2AD systems for deny, delay, disrupt, destroy, or manipulate (D4M) effects. The 915th and MDTF can contribute to investigating and developing A2AD solutions and D4M capabilities. Tough challenges of investigating and deep familiarization of adversary A2AD capabilities and systems can lead to discovering weaknesses in development, functionality, or employment enabling countermeasure development or OCO and EW exploitation opportunities.

For the unit to successfully achieve its goals, accomplish its tasks, and execute its unique mission, the organization will develop relationships with its supported tactical counterparts at all echelons to ensure that its capabilities are understood. The 915th must be engaged during the competition phase to provide demonstrable effects in the conflict (penetrate, disintegrate, exploit) stage. It is unrealistic to expect cyber operators to provide effects against an adversary in conflict without having conducted appropriate operational preparation of the environment. Cyber operations require investment of significant time and resources devoted to developing employable courses of action for commanders. An ECT must evaluate and gain situational awareness of terrain to assess and plan avenues of approach, identify capability needs and development requirements, and identify optimal targets to enable effective cyber support to corps and below. To accomplish these objectives, the unit will continue to work to establish and strengthen relationships with supported commanders. Both battalion and ECT leadership will establish and leverage relationships with supported Combatant Commands, Multi Domain Task Forces, Cyber Operations-Integrated Planning Elements, and Joint Cyber Centers to understand and gain their projected conflict requirements. Obtaining these requirements are necessary to form the basis of the 915th's competition mission. Armed with requirements from the force, the CWB can work through US Cyber Command's Joint Forces Headquarters to obtain necessary authorities to conduct Intelligence, Surveillance and Reconnaissance (ISR) during competition to prepare for conflict support. The promise of the ability to convert requirements from U.S. Army supported corps and below tactical forces into actionable information warfare operations is one of the aspects that makes the 915th special. As ECTs become regionally aligned and are integrated through each echelon, developing partnerships, and assisting tactical counterparts understand Information Warfare capabilities, authorities, and processes will enable mission success.

The 915th is a service retained unit under ARCYBER, but refining interaction and authorities processes with each of the services' Joint Forces Headquarters – Cyber (JFHQ-C), U.S. Cyber Command (USCC), and ARCYBER is of paramount importance for future operationalization. The 915th derives its ability to conduct sensitive cyber operations by leveraging authorities from various partners. The authority to conduct tactical cyberspace effects operations is derived from Combatant Command EXORD/OPORDs. The authority for the 915th to conduct cyber-enabled ISR and S&R operations in the competition phase is derived from USCC. Service-aligned USCC JFHQ-Cs are further aligned to areas of operations that the 915th may operate in. This requires the 915th to refine coordination processes with the various service JFHQ-Cs to turn the requirements obtained from the supported tactical force into USCC approved mission profiles authorizing C-ISR and C-S&R operations. As previously noted, to maximize effectiveness for ECTs in conflict, preparations in competition are essential. This demands obtaining conflict requirements from the force and translating them into C-ISR and C-S&R mission profiles. Organic ARCYBER DACO authorities are for DoDIN operations and do not arm the 915th appropriately to accomplish its unique expeditionary OCO mission. Refining governing authorities and COMREL is of utmost importance moving forward for the 915th to accomplish its objectives. This is not limited to offensive cyber authorities. The 915th will also continue to work to fully establish its organic intelligence capabilities to perform analysis and production in support of its OCO,

EW, and IO missions.

The 915th CWB has come a long way in three years. The unit participated in Defender Europe, Defender Pacific, and conducted a validation exercise for an ECT at Muscatatuck Urban Training Center (MUTC) in Indiana with plans to hold at least two validation exercises per year moving forward. These experiences have helped the organization develop and hone TTPs for the CEMA fight and offered opportunities for learning and growth. The future for the 11th Cyber Battalion is both challenging and bright due to the work and sacrifice of the pioneers of the 915th who have fought through three hard years of discovery learning. ■

References:

(2018). TRADOC Pamphlet 525-3-1: The U.S. Army in Multi-Domain Operations 2008. U.S. Army Training and Doctrine Command.

Task Force Echo Warrant Officers Make a Distinct Mark

By CW3 Teri Walker and CW4 Dustin Lee, Task Force Echo 6, Senior Technical Advisors

Introduction – Warrants within the Task Force

SINCE 2017, THE ARMY NATIONAL GUARD has supported U.S. Cyber Command by mobilizing Soldiers to serve as part of Task Force Echo, a support element to the 780th Military Intelligence Brigade (Cyber), headquartered at Fort Meade, Maryland. Additionally, since 2019, the Guard has had a contingency operation supporting Joint Force Headquarters–Cyber at Fort Gordon, Georgia. On the current rotation, the sixth of its kind, 33 Warrant Officers serve as technical experts and advisors across all sections of the Task Force. They hail from Indiana, Georgia, Louisiana, Mississippi, Kentucky, Texas, Florida, and Virginia, ranging from Warrant Officer 1 to Chief Warrant Officer 4, and work as Developers, Data Scientists, Exploitation Analysts, Infrastructure Engineers, Forensic Engineers, and Requirements Program Managers. Though the TFE mission may eventually end, the indelible mark of National Guard Warrant Officers is undeniable in the history of the Army Cyber branch and the 780th MI BDE.

The best industry has to offer on loan to the Army

When not in uniform, many of these Chiefs work in the private sector, perfecting their craft and solving large-scale enterprise challenges for industry leaders such as Booz Allen, Accenture, PricewaterhouseCoopers, Elastic, RSA, SecurityOnion, Truist, Circadence, Primerica, and KAR Global. They fill roles as programmers, principal architects, data scientists, network security engineers, server development engineers, and cyber security engineers; their diverse career experiences add a distinct perspective to help build solutions aligned with strategic objectives.

For example, CW3 Joshua Adams works as a security architect for a global enterprise maintaining responsibility for the security of multi-cloud and on-premise IT systems. He collaborates across 17 lines of business to achieve security and business objectives, such as vulnerability management and source code objectives. Since arriving at the 780th, he has leveraged his skills in architecture security and best practice firewall configuration to help build and secure network architecture supporting the Joint Mission Operations Center's (JMOC) infrastructure.

CW2 Dale Lofton completed a Computer Network Operations course to learn about operating system software protection and exploitation in his civilian position. With his knowledge of OS kernels, vulnerabilities, impact surface areas, and troubleshooting steps, he could construct automated defensive-focused administration tools that perform forensic interrogation, hardening, and decommissioning.

"As a lifetime systems administrator, I learned more about operating systems than I ever thought was possible in this course," said Lofton. "I was able to take that knowledge and implement those techniques into this tool to help increase efficiencies and reduce the threat surface attack area in support of cyber operations."

His efforts have served as a foundational framework for other automation tools deployed throughout the infrastructure.

Networking across the WO cohort to solve complex challenges

You may have heard the moniker "Warrant Officer Mafia" before – it rings true within the walls of the 780th. As we are spread across all sections of the Task Force and touch every facet of operations, we call on our cohort to rapidly build small, informal, technical teams from those sections to develop multifaceted solutions in true "skunkworks" fashion.

CW2 Jason Childers says, "in the JMOC, I've had to call upon the cohort from other sections to meet critical short-term requirements to support mission executions, leveraging networking and soft skills to bring people together to solve complex problems. The biggest thing I have learned in my civilian job that helps me in my current position is that everything is a people business. Even in a high-tech cyber environment, interpersonal relationships are a necessity. Working for private industry, I learned how to establish teams on the fly to achieve desired outcomes"

WO1 Matt Do attributes his civilian experience working as a Vulnerability Analyst and Data Scientist as a motivating factor to build skills to support an automated Machine Learning/Artificial Intelligence pipeline to perform reverse malware engineering and system patching. Matt's civilian job allows him to work as part of a team to develop capabilities that identify platform security threats earlier than commercial off-the-shelf products through automation. As the lead python developer for Task Force Echo, he is often called on to assist with various projects requiring rapid prototyping across a broad spectrum of focus areas. Leadership recognizes Matt's expertise as a force multiplier, specifically programming, ML, and pipeline development. He directly impacted force structure changes and resource support, mitigating potential negative impacts on operations.

Beyond the JMOC – Warrants breaking barriers in the 147th Cyber Warfare Company (CWC)

Thanks to significant efforts by the 780th WO cohort: CW3 J.P. Dixon,

WO1 Ensor Sierra-Mercado, WO1 Freddie Weeks, and new WO1 Mark Outlaw, the 147th CWC transcended impediments that the Guard faced conducting offensive cyber operations independently of COMPO 1. CW3 Dan Marr and CW3 Shari Simzyk harnessed their vast knowledge and expertise in network security and threat emulation from training, certifications, and private industry work to become T10 JQR (Joint Qualification Record) qualified as Exploitation Analysts; a first for National Guard Soldiers. To significantly improve the current and future CWC efforts, CW2 Steve Jamison led the endeavor to document and promote an effective knowledge management program, leading to well-built, approved, trained, delegated, and maintained documentation for future CWC handoff. This new pipeline paves the way for future COMPO 2 support in OCO billets and qualifies the team to conduct future planning and execution of offensive cyber operations.

Leveraging Task Force Echo as a springboard to enhance individual career growth

Like all Soldiers transitioning, as we start to draw down on this mobilization, we will go through the Transition Assistance Program, building resumes highlighting our previous work experience. For most of us, we have secure positions to return to, but the opportunity to level up in a new role or with a new company by capitalizing on the skills built during the mobilization is appealing. CW2 Hill states that during his two tours in the JMOC, he has strengthened his analytical and investigatory skills and is excited to showcase new persistent hunt techniques when he returns from mobilization.

Our Active Duty counterparts spend most of their time perfecting their craft in the branch, but a broadening assignment may mean a stint in Recruiting or as a TAC Officer. For TFE Warrant Officers, their broadening assignments support worldwide industry leaders facing dynamic challenges in our civilian positions. This cycle lends to a higher job trajectory curve versus solely attending Army work role training, PME, and defined work role experiences. These mobilizations allow them to pinball back and forth between Army & private industry, promoting continued growth and networking amongst the cohort.

Taking a page out of TFE second-timers' book, CW3 Dan Marr and CW3 Julius Wilson spent their first mobilization engineering and deploying ElasticStack at an enterprise scale. Shortly after returning home, they were brought onboard Elastic as architects to capitalize on their expertise. For these Warrant Officers, the professional appetite for more and striving for technical excellence inspires their volunteer service.

Making the sacrifice worth it

If you ask a National Guard Warrant Officer why they continue to mobilize on a three to four-year rotational cycle to support Task Force Echo, most will tell you they can work with their peers from other industry leaders. Opportunities to collaborate, learn from, and grow professionally, given the scope of work within the 780th, do not cross over into private industry on a one-for-one basis. They choose to sacrifice time with family and civilian careers to bring the best skills they have to offer to Active service. As the Army continues to grow as a force in the cyber domain, the Warrant Officer cohort will grow as individuals and collectively to solve complex and dynamic challenges to support USCYBERCOM's cyber operation objectives. As an old National Guard Warrant Officer once said, "You have many gems in the formation; placing them in a position to shine allows us to forge paths we never knew could exist." ■

131A Field Artillery Targeting Technician in Cyber Today

By CW3 Mark A. Horton, Cyber National Mission Force Deputy Chief of Fires

"I do not need to tell you who won the war. You know, the artillery did." – George S. Patton

Past:

THE FIELD ARTILLERY TARGETING TECHNICIAN (131A) positions were established in U.S. Army Cyber Command (ARCYBER) and the 780th Military Intelligence Brigade (Cyber) to serve as the primary advisor to the commander and staff on all matters relating to the employment of cyberspace effects operations (CEO), the Joint Targeting process, and methodology.

131As were aligned to positions at all echelons from tactical, operational and strategic levels and were labeled as a critical billet resulting in the creation of fifteen slots embedded across Staff, National Mission Teams (NMTs), National Support Teams (NSTs), and Combat Mission Teams (CMTs).

To maintain tradition, listed below are the 131As whom have served in a Cyber role since its establishment. These Artillerymen have been charged with instituting the groundwork of the 131A in Cyber, and to continue pushing the positions in an innovative manner from a Cyber and Fires standpoint:

CW5 (ret) James Jeter
CW5 (ret) Lynn Weatherspoon
CW5 (ret) Bob Tisdale
CW4 (ret) Thomas O'Neill
CW4 (ret) Jaime Mannings
CW4 (ret) Shomara Anderson
CW4 (ret) Andre Stewart
CW4 (ret) Ted Dimone
CW4 (ret) Kris Williams
CW4 (170A) Nolan Reed
CW4 (170A) Chad Mastbergen
CW4 Jordan Kness
CW4 Jerome Isaac
CW3 (ret) Anthony Preston
CW3 (ret) Scott Clark
CW3 (ret) Vince Wolterman
CW3 (ret) Will Figueroa
CW3 (ret) Tim Wing
CW3 (ret) Pete Green
CW3 (ret) Steve Harrell
CW3 (ret) Richard Westmoreland
CW3 (ret) Dave Cutler
CW3 (ret) Jeff Bisel
CW3 (ret) Mike Hill
CW3 (ret) Robert Greenleaf
CW3 (ret) Jason Brown
CW3 (ret) Nick Burt
CW3 (ret) Harry Burgess
CW3 (ret) Edwin Villanueva
CW3 (ret) Dan Hatfield
CW3 (ret) Baron Claytor
CW3 (ret) Michael Holdway
CW3 (170A) Dustin King
CW3 (170A) David Aresco
CW3 Darryn Sampson
CW3 Josh Swan
CW3 Jose Gomez
CW3 Eddie Rivas
CW3 Patrick Knowlton
CW3 Mark Horton
CW3 Phillip Merriam
CW3 Morgan Durham
CW2 (ret) Jacob Klassen
CW2 Nolan Laughlin
CW2 Adam Connolly
CW2 Eric Rondeau
CW2 Nikolaos Arenas

Targeting is the process of selecting and prioritizing targets and matching the appropriate response to them, considering operational requirements and capabilities. –JP 3-60

Facilitates the development, integration, synchronization, and execution of CEO, Information Operations / Military Information Support Operations and Special Technical Operations (STO) targets in support of plans for Global Crisis and Contingency Operations.

Integrates Target development nominations for inclusion to the U.S. Cyber Command (USCYBERCOM) JTL/RTL (Joint Target List / Restricted Target List) through collaboration with the Intelligence Community.

Represents Army Cyber in joint, interagency, and international working groups and conferences that includes Cyberspace targeting, Joint Fire Support, and threat mitigation related planning considerations.

Establishes a quarterly process for targeting guidance and prioritizing the development for targets in support of multiple objectives and effects for the Joint Planning Process.

Synchronizes and coordinates the Joint Targeting process, Joint Fires planning, and Joint Fires in support of objectives and effects across future plans and future operations at all echelons.

Present:

131As applying their foundation in doctrine work tirelessly in the identification and establishment of key Standard Operating Procedures (SOPs). To date the 131As have written, established, and solidified documents covering dynamic targeting, target

development, and collateral effects estimation methodology for cyberspace. The dynamic targeting SOP outlines the procedures and framework for cyber domain unique requirements to execute CEO dynamically due to operationally pertinent appropriateness. It provides the structure for rapid identification, deconfliction and execution of cyberspace operations. The 131A utilizes the chairman joints chief of staff instruction (CJCSI) 3370.01C Target Development Standards and joint doctrine for targeting with four intelligence community agencies to develop, de-conflict, and employ effects in accordance with the USCYBERCOM Commander's objectives and effects as well as in support of other Combatant Commands. They participate in the joint staff updates and rewrites to ensure cyber domain uniqueness is codified and understood throughout. To ensure the Commander can understand risk during executions, the collateral effects estimation methodology for cyberspace (CEEM-C) was outlined. CEEM-C is a repeatable process for the identification of collateral effects and control measures of employment capabilities.

Doctrine helps establish the foundation, and Cyber Training Exercises (CTE) codifies the processes being implemented. The 131As participate as Brigade assessors, for the Fires Planner, and Joint Targeting Analyst job roles. In these positions the 131A trains and evaluates individuals to meet the joint qualification requirements. Post exercise we transition to the curator role and make necessary adjustments and upgrades to both the Joint Qualification Records (JQRs) and exercise design to ensure we are always training how we fight. This has resulted in three individuals obtaining the master level fires planner.

Outside of CTEs' the 131A is training future mission commanders through teaching at the mission commander's course. We provide a general overview of the six-phase iterative joint targeting cycle (JTC), while highlighting key inputs and outputs of each phase of the JTC to ensure future mission commanders have a better understanding of how their future missions nest in the Commanders objectives and effects.

Operationally 131As are synchronizing/implementing these processes in real-time. Ensuring the organization is continuing to remain an effects-based organization. They have been vital to the development and execution of over 20 cyber effects operation mission packages that have been presented to inter agency partners, combatant commands, and the Secretary of Defense and POTUS.

Targeting requires a continuous, analytic process to identify, develop, and affect targets to meet commander objectives. –JP 3-60

Future:

The Field Artillery Targeting Technician is a highly sought out individual in all formations throughout the Army, and 131As in Cyber organizations are absolute force multipliers. While the Field Artillery Branch continues to work to fill the critical 131A billets throughout the Army, the senior 131As in Cyber will continue to participate in vital events that help to highlight the necessity of filling the Fires Planner billets, with 131As. Recently, the Field Artillery Symposium provided an opportunity to sit down and discuss this necessity with key leaders such as the Field Artillery Chief Warrant of the Branch CW5 Rios and the Field Artillery Proponent Officer CW3 Zamora. Providing these vital leaders, with a better understanding of the personnel operating in Cyber to articulate the necessity of prioritizing these critical billets.

We will continue working on refining the Fires planner JQR back to the USCYBERCOM authorized job roles. The upcoming Fires planner Cyber Standards Analysis Team (CSAT) will address key areas in which should be added and trained for individuals qualifying as a Fires planner. ■

Author: Chief Warrant Officer 3 Mark A. Horton currently serves as the Cyber National Mission Force (CNMF) Deputy Chief of Fires. He holds a JQR in Fires Planner (Master). He has 18 total years of Fires experience and has been a part of the 781st MI Battalion since 2019. He holds a Master of Science in Management, Strategy, and Leadership from Michigan State University.

A Broadening Opportunity (255S)

By CW4 John Rolley, 781st MI BN (Cyber), Malware Analyst Cell OIC

UNDENIABLY THE WORLD IS BECOMING INCREASINGLY more interconnected. As the world evolves and Globalization is the new norm, we must embrace change and face the unique landscape with our eyes wide open. The internet has allowed the world to link together in ways never seen before. We are enabling communication and collaboration with people worldwide. Globalization has changed the fundamental way we see the world and how the world views us as a nation. Due to this ever-growing and continuously evolving landscape known as the internet, we have enabled countries worldwide the ability through cyberspace to reach out and touch the U.S. whenever they wish. Unfortunately, the nature of conflict has changed since the old "Cold War" days. Both state and non-state actors will continue to develop a greater capacity for stand-off and remote attacks. Growing development of cyberattacks, precision-guided weapons, robotic systems, and unmanned weapons lower the threshold for initiating conflict because attackers put fewer lives at risk in their attempts to overwhelm defenses. The proliferation of these capabilities will shift warfare from direct clashes of opposing armies to more stand-off and remote operations, especially in the initial phases of conflict (NIC, 2017).

Cybersecurity is the greatest threat to our national security from nation-state adversaries who want to harm us. As part of our mission area to "Defend the Nation," United States Cyber Command is the only agency in America that has the legal authority to "fight back" in case of a significant cyber-attack by a foreign state actor or terrorist organization, or cybercriminal group.

On March 25, 2021, GEN Paul Nakasone testified to the Senate Armed Services Committee that the United States has a 'cyber blind spot' by stating:

"We may see what's occurring outside of the United States, but when it comes into the United States, our adversaries... understand the laws and the policies that we have within our nation, and so they're utilizing our infrastructure, our Internet service providers, to create these intrusions... "It's not the fact that we can't connect the dots. We can't see all of the dots."

Adversaries leverage ransomware to disrupt critical infrastructure around the world. Malware continues to be an easy avenue for threat actors of all skill levels to generate revenue or gain a strategic advantage. The amount of malware in the wild will likely continue to increase, with much of it sharing similar code due to code reuse, despite attempts at obfuscation. Modern security solutions use various techniques to identify static malware, including signature-based and heuristic detection. While these solutions offer some protection, they may struggle with unidentified instances or variants of previously identified malware. However, we have an imminent need now more than ever for collaboration across all levels of government to share indicators of compromise and enhance visibility across the nation (Cythereal, 2022).

Next came the vision and implementation of the ability to synchronize collaboration across all 50 states with the analysis of malware with the National Guard, resulting in better visibility of cyber threats across the U.S. Then, develop related indicators of compromise for the National Guard and the Federal Government's use to strengthen the nation's cybersecurity posture. This level of collaboration and feedback provided local, state, and DOD partners with a holistic view of threats occurring in the United States. Following the discoveries of foreign influence in U.S. elections, USCYBERCOM needed information exchange capabilities. With the ability to collaborate on cyber incident information with the National Guard and federal mission partners supporting the cyber defense of state and local government networks. The Command developed an effective Information Exchange Program called Cyber 9-Line to submit cyber incident data to address this mission need. This data includes malware files and indicators of compromise and provides the Command with valuable data for cyber planning, defensive operations, and diagnosing a foreign attack further while delivering timely, unclassified feedback to the victim. Cyber 9-Line enriches state and local cyber self-defense and USCYBERCOM's persistent engagement activities by enabling analysts to access USCYBERCOM's unclassified Big Data Platform or BDP. It increases a mission partner's cyber-self-defense through access to a massive (petabyte-scale) consolidation of information that can be analyzed using configurable analytics, artificial intelligence, and machine learning.

The Cyber 9-Line program is supported through a few essential technologies:

- Unclassified BDP portal accessible to federal and state mission partners via CAC/PIV
- USCYBERCOM's BDP for the capture of Cyber 9-Line submissions
- TeamWorx HIVE-IQ as an INTERNET accessible, a commercial platform used as a secondary input mechanism for non-CAC/PIV access
- Rapid USCYBERCOM and HIVE-IQ malware analysis to develop deployable indicators of compromise to defend and protect the DODIN and the nation

As I wrap up my tenure here in 780th Military Intelligence Brigade (Cyber) as a 255S, gaining the knowledge and experience working alongside my offensive cyber brothers and sisters has been my career's most challenging and extremely rewarding experience. The initiative's success mentioned above hinged upon

Continued on page 14

SIGINT in Cyber (352N)

By CW3 Zachary Hofstra, 782d MI BN (Cyber) and CW2 Lonnie Robinson, 781st MI BN (Cyber)

SIGINT (SIGNALS INTELLIGENCE) WARRANTS are pivotal to requesting, collecting, and disseminating actionable intelligence to enable cyberspace operations. They enforce Intelligence Oversight and train individuals and teams on the best analytical practices. 352Ns are a crucial component of the future success of the cyber mission and should be fully manned and have longer terms in cyber.

352Ns use their previous experience and knowledge to advise and assist leadership on enemy tactics, techniques, and procedures to identify potential vulnerabilities within adversary networks. They collaborate with cyber planners to find possible avenues of approach to counter cyberspace actors and collaborate with operations sections to provide actionable intelligence to reach commanders' end states. 352Ns lead analysis and production shops to answer customer needs, aid potential target nomination, and enable continuous cyberspace operations.

SIGINT Technicians make sure post-operation information is reviewed, validated, and reported by analysts. 352Ns enforce continued collaboration between analysts and other intelligence community members by analyst-to-analyst exchanges, partnerships, and production. 352Ns mentor and train Cyber and Military Intelligence (MI) Soldiers on the best analytical practices to guarantee intelligence compliances are met. Additionally, 352Ns increase their own, and the brigade's spheres of influence by becoming assessors and adjunct instructors. Intelligence Oversight is a legal policy requiring analysts to understand their mission scope, target, and established toolsets. Compliance functions are essential to daily practices and failures could result in a loss of missions, authorities, and accesses.

Warrant Officers are supposed to be the subject matter expert, but unfortunately, cyber requires knowledge not necessarily used in any other realm. A three-year tour does not nurture the growth of knowledge. Civilians have always served as the unit's continuity, but shouldn't that be the job of the Warrants? Warrants should provide target and policy continuity and should be assigned to multiple billets within cyber. Increasing the time on the ground would allow 352Ns to become versatile and aware of the ever-changing cyber requirements. The MI branch should enable individuals who fully understand how to support real-time cyberspace operations to extend and nest inside cyber mission teams by conducting a longer-term PCS cycle in cyber or promoting back-to-back tours inside of cyber missions. ■

Continued from page 13

the differing equities of each. Possessing a defensive cyber background and being immersed in the offensive cyber arena has been a phenomenal learning opportunity.

References:

Cythereal is the leader in predicting and preventing advanced malware attacks. cythereal. (n.d.). Retrieved May 20, 2022, from https://www.cythereal.com/

NIC, (n.d.). Paradox of Progress. Office of the director of National Intelligence - Global Trends. Retrieved May 20, 2022, from https://www.dni.gov/index.php/gt2035-home. ■

The Electronic Warfare Technician: Bridging Cyber Space Operations via the Electromagnetic Spectrum

By WO1 Tye Cowher and CW2 Rob Tarkington, 915th Cyber Warfare Battalion

While the Electronic Warfare (EW) community has a significant history in our Army, the career field was disbanded after the end of the Cold War and re-instated in 2008 in response to the Radio Controlled Improvised Explosive Device threat from the Global War on Terror. Fast forward 14 years, and EW is integrated into all aspects of Army Multi-Domain Operations at each echelon from tactical maneuver Brigades, through Army Service Component Command and most recently the Cyber Force. While the integration into Cyberspace Operations (CO) is still a relatively new concept, the 780th Military Intelligence Brigade (Cyber) is spearheading the effort via units such as the 915th Cyber Warfare Battalion with EW personnel located on each of its Expeditionary CEMA teams.

The EW Technician, 170B, traditionally resides on staffs at the brigade through Combatant Command (CCMD) echelons, and functions as both the equipment subject matter expert and external capability integrator. However, in the 780th, EW techs have been called on for a unique role that they traditionally do not support. This includes EW operations such as special purpose and standard electronic attack missions, EW support functions, and electronic protection measures in support of expeditionary CO. With these requirements, EW Techs are integrating new capabilities with supported units to both educate, implement, and bridge CO with tactical-edge units by providing effects generally unavailable to maneuver operations.

EW Techs in the 780th have access to unique and premier EW equipment allowing them to support all facets of CO, be it creating radio frequency networks for Expeditionary Cyber Operators to utilize or conducting denial operations against hostile emitters to support maneuver operations. They conduct EW Support operations to identify both friendly and adversary emissions and pinpoint them on the globe, establish required range for effective Spectrum Enabled Operations and conduct protection missions to mitigate friendly vulnerabilities that may exist in the electromagnetic spectrum.

EW Techs also have an inherent responsibility to coach, mentor, and educate cyber leaders and operators. Often called on to help identify new and emerging capability requirements, facilitate integration into foreign nation spectrum environments, and prepare concurrent unit level EW concepts and equipment training. We often serve in roles of Jam Control Authority and provide inputs to Joint Qualification Records, Joint Qualification Standards, and Tool Qualification Standards, helping to further integrate Electronic Warfare into Cyber Space Operations within the Brigade, and across the Army! ■

"Street-to-Seat" Refining the Warrant Officer

By CW4 Phillip Smith, 780th MI BDE (Cyber), Cyber Solutions Development

A WARNING TO THE READER. This an opinion piece. My hope is to generate thought within the community, and I welcome any feedback or thoughts on this subject!

My first encounter with a Warrant Officer was surely an interesting one. I was a Specialist and an infantryman in a light infantry company. On a rather boring day, my boss sent me down to the motorpool to dispatch the commander's vehicle. When I arrived at the MP, I discovered the only person in the shop was the Battalion's Maintenance Tech, or more lovingly, "Chief". Despite hearing many legendary tales about the guy, I had zero idea what a Warrant Officer was. All I knew was he could somehow magically disappear into the wind, literally speak to HMMWV engines, and his word on the Battalion's maintenance status was basically law.

I knocked politely on the shop office half-door, more than a little terrified. "What do you need, troop?" he asked. I explained that the commander wanted a vehicle dispatched. "Happy to help with that. I need to take care of one thing first." He then kicked back in his chair, reached into his bottom desk drawer, and fetched an electric razor. He then shaved for about 5 minutes, all the while he stared at me. He put the razor away, closed the drawer, hopped to his feet, and said, "Okay, about that vehicle!"

Over the next few years, I had many more encounters with Chief. I learned quickly that, despite the quirky shaving incident, the legends were true. His expertise with vehicles was off the charts. However, he was much more than just an engine whisperer. He never missed an opportunity to mentor and teach. He shared every bit of his vast knowledge and experience freely. The commanders respected him and sought his advice on maintenance of their vehicles. He cultivated a vast network of Warrant Officers and leveraged them to acquire things quickly and grow in his craft. He knew how the Army really worked and how to navigate the various background channels. Through him, the Battalion achieved maintenance excellence and top-notch readiness.

Despite taking a wildly different Warrant path, I credit this Chief with my desire to become a Warrant. He also set the bar for what I desire to see in my fellow Warrants and potential candidates - *A Warrant Officer is not only a technical expert, but also a mentor, a trainer, an advisor, and is deeply networked within the Army.*

Army Pamphlet 600-3, paragraph 3-9, says this: "The Army warrant officer is a technical expert, combat leader, trainer, and advisor. Through progressive levels of expertise in assignments, training, and education, the warrant officer administers, manages, maintains, operates, and integrates Army systems and equipment across unified land operations. Warrant officers are innovative integrators of emerging technologies, dynamic teachers, confident warfighters, and developers of specialized teams of Soldiers. They support a wide range of Army missions throughout their career. Warrant officers in the Army are accessed with specific levels of technical ability. They refine their technical expertise and develop their leadership and management skills through tiered progressive assignment and education."

Keep those definitions in mind.

Last year, the Army created its first few Cyberspace Capability Technicians through the VTIP process and kicked off the first 170D Warrant Officer Basic Courses. Our collective goal to create approximately six new 170D Warrant Officers per year. Most importantly, the Army made one very interesting proposal regarding the creation of 170Ds. The Army worried about finding enough technically strong candidates to meet recruiting objectives and opened the door for direct accessions into the cohort. A program heavily used by aviators called "Street-to-Seat" or S2S.

This brings me to the heart of this discussion. Will recruiting technical Warrant Officers through S2S change the definition of a Warrant Officer?

Recently, a junior developer recently asked to write a letter of recommendation for them for 170D. This candidate was already a certified basic developer. However, they were missing the other facets that draw the distinction between budding senior developer and Warrant. They were inexperienced in mentorship and fresh to the Army. They were not yet ready to advise or assist a commander. They had not yet had a chance to learn the intricacies of how the Army runs. So, I declined to write the letter of recommendation and instead provided a series of milestones to work toward that would earn them a letter next time. I reflected on this decision a lot. It weighed heavily on me because I knew we were simultaneously moving towards a S2S option. Was I wrong to refuse this soldier a letter when we will in the future recruit an unmeasured candidate direct from the street?

I don't believe I was wrong. Given enough time, the S2S recruitments, at least in the case of Cyber Developers, will change the definition of what it means to be a Warrant Officer. This effect will be accelerated the more heavily we use S2S over internal accessions. We will undoubtedly find highly talented civilians, but I believe it will be especially challenging to find technically talented civilians that have the necessary Army experience that makes the Warrant Officer so unique and capable.

It is my opinion the best course of action is to avoid the S2S option and only pursue it if necessary to maintain minimal readiness. When used, the selection process should be deliberate and tailored to find the very best candidates that not only have technical depth but the key characteristics that make Warrant Officers special. Our primary goal should be to grow talent from within and preserve the trust and respect over 100 years of Warrant Officers have created for the cohort. I welcome any thoughts or comments on this topic. ■

PCTE: Liberation from the Training Paradigm

By CW2 Richard Soto, 781st MI BN(Cyber), S3 Training and Exercises OIC

TRAINING, IT IS A GIVEN IN THE ARMY, RIGHT? Ever since our start in the service, we are being routinely and systematically trained to a series of standards to ensure we fulfill our role in the mightiest force in the world. In many cases, we take training for granted. It is so ingrained in our culture that every October we mentally prepare ourselves for another round of mandatory training. Training is highlighted further when we consider the enormous cost and effort the Army undergoes to prepare us as Cyber Soldiers. Upon joining the unit, work-role pipelines are our sole focus. We dedicate ourselves to completing the required courses and pouring over the necessary training. Why is it then that once we have finished our pipeline, training emphasis seems to fade? We become so operationally focused that our priorities shift. It would stand to argue that considering the rapidly evolving nature of Cyber we should be constantly seeking opportunities to research, refine and retain.

There is a training void that is keeping us as a force from reaching new levels. To keep our Cyber sword dynamically sharp, on-the-fly technical hip pocket training, readymade small group ranges, rehearsal scenarios, intelligence fundamentals, language training, organizational specific training and more should be accessible on a whim. We should not wait for a contractor, vendor or agency to build and deliver what we can do ourselves. Warrant Officers are the primary group that should be leading the initiative to provide this high quality, realistic, repeatable training to our small groups and teams. Being the technical experts, driven by passion for learning and dedication to the mission, Warrant Officers are the ideal stewards. As a collective, Warrant Officers can combine their years of operational experience, technical prowess, and influence as leaders to deliver on this critical need.

All training requires the allocation of some type of resource, whether it be human, material, or financial. The Persistent Cyber Training Environment (PCTE) is the platform that delivers most of those resources at little to no cost to the end user. Many have had some degree of exposure on to PCTE, yet for those who have not, PCTE is a large-scale virtualized training environment offered to the Department of Defense. PCTE consists of a series of regional datacenters with instances on the unclassified internet (accessible from any CAC enabled computer) and Top-Secret instances. The platform provides a means to conduct large scale events such as Cyber Flag but also can deliver on-demand individual training, rehearsal, testing and more.

PCTE Technical Features:

- Rapidly scalable environments
- Automated Host configuration
- Simulated Internet, User activity, and attack campaigns
- Internal OS repository mirrors
- Vast library of native and user create virtual machines (VM)

In addition to excelling at realistic virtual environments, PCTE can deliver training beyond technical scenarios. The built-in Learning Management System can facilitate almost any subject matter, whether it be abstract, information based, or highly technical.

PCTE Learning System Features

- Historical Training Records
- Leaderboards & rating feedback system
- Robust training development framework
- Competency framework mapping
- Organizational training metrics and tracking

For some who have used PCTE, it might feel like a novelty, something that is only useful occasionally, for exercises or simulations. Without deeper exposure, the platform could appear fairly one dimensional. After investing time with PCTE our veteran users can attest to the flexible and dynamic nature of the platform. Mr. Ken Burcaw, Cyber Range Systems Administrator, and primary range builder for the 782nd MI Battalion, touches on how PCTE has impacted his battalion (BN):

"As a platform, PCTE provides the BN with a highly flexible training environment. … The vast library of VM choices, user, and traffic generation, allows trainers and rehearsal range builders all the tools needed to make the environments feel like a live network. PCTE's v4 update has also introduced a self-paced, auto-graded, training allowing for operators to progress from Basic to Senior to Master at a better pace."

CW2 Arsenio Pagan, a highly experienced PCTE engineer and developer of the PCTE T10 Basic Operations Course range, said:

"The Persistent Cyber Training Environment (PCTE) has by far been the best Cyber Training platform provided during my time in service. It allows you to create realistic training for any situation and can replicate any training or rehearsal scenarios that you may want to emulate. PCTE is capable of housing any software that you can get your hands on."

Another senior PCTE engineer CW2 Christopher Ryan, the primary technician responsible for the execution of the CNMF Task Force collective exercise, said:

"The Persistent Cyber Training Environment (PCTE) … is able to facilitate the largest range of virtual learning, range management and virtualized networking available in a single platform. Currently, its use varies from virtual training lanes to defensive forensic exercises, as well as offensive operational training and rehearsals. …PCTE is able to perform concepts currently

not available in other platforms, ranging from user emulation and traffic recording to virtual machine template reuse and network blueprinting."

Further highlighting the power of PCTE, SFC Joshua Stockman, a Senior Operator and premier range engineer, discusses how PCTE requires our investment to maximize its value:

"PCTE brings us the platform for training and mission rehearsal that we have been lacking for years. While there is a learning curve, PCTE ranges can easily be shared across users and perform advanced simulations. We need to invest the time in building these ranges and training users on the platform. Doing so will help streamline JQR completion, provide simulated target environments for mission rehearsals and familiarize users with the platform for exercises."

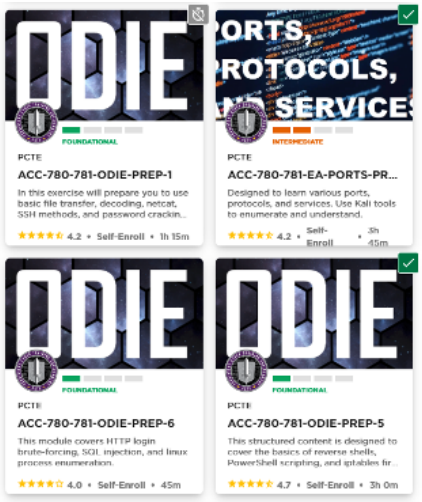
WO1 Sir Addison, a mission critical Cyber Operator and trainer, helps us further understand the incredible potential PCTE offers:

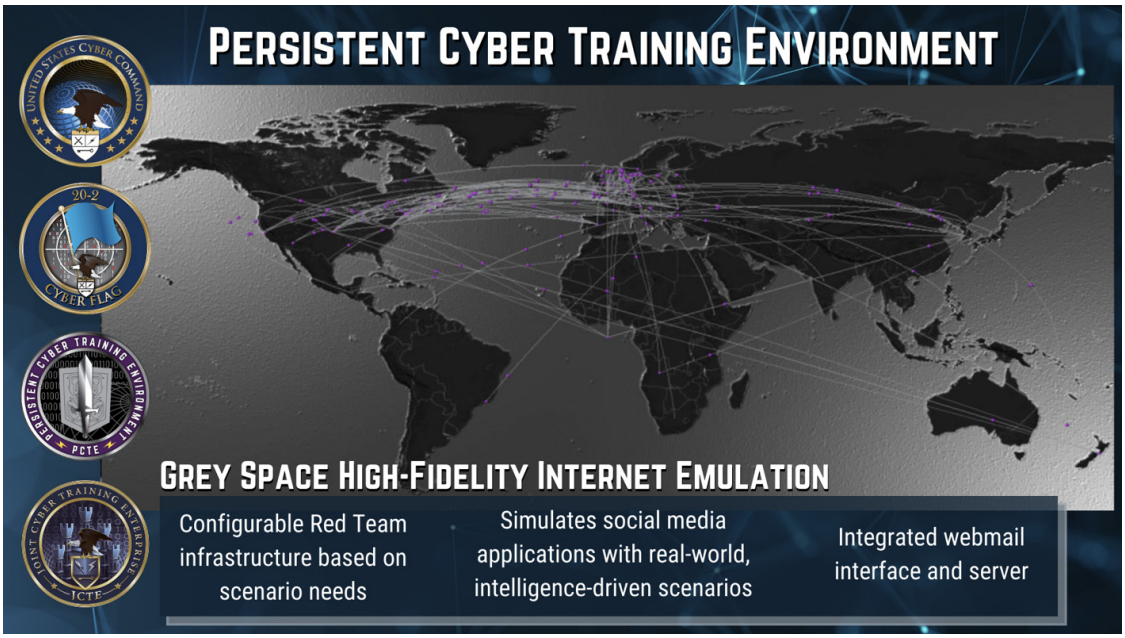
"Persistent Cyber Training Environment (PCTE) enables future Operators to experience and rehearse mission plans … we digest the requirements and build a platform that completely mirrors the fighting environment. … The ability to produce a full network under an hour should be the standard and PCTE delivers that as an option. PCTE supplies the ability to practice new techniques, confirm tool usage and replicate live problems resulting in real-time solutions without added risk. … I encourage all team members to practice and rehearse plans through PCTE, it is truly a top-tier platform for training."

Lastly, CW3 John Graber, the 780th MI BDE TREX OIC and individual responsible for brigade exercises and evaluations, recants how PCTE has impacted the unit's abilities:

"The Persistent Cyber Training Environment (PCTE) provides the Cyber Mission Forces (CMF) the ability to conduct individual and collective training exercises and mission rehearsals in a stable and realistic environment and share content across organizations. Training within PCTE is easily customizable, reusable, and replicated reducing overall time and resources dedicated to content development while increasing accessibility contributing to individual and unit readiness."

In the 781st S3 TREX we strive to further the training initiative in any way we can, whether that be through facilitating accounts, platform training, content development, or resource allocation. We encourage subject matter experts in our formation to engage us to facilitate training aspirations and begin to fill the critical need for high quality, relevant, and accessible Cyber training. By those directly engaged in current operations developing content, we ensure training outcomes are direct representations of the knowledge, skills, and abilities required of Soldiers on mission. The fact is, we stand on the precipice of new era, where we as a force can develop and deliver high quality, dynamic, timely, and diverse training without reliance on third party entities to meet our needs. Taking this into consideration, the question remains, what can you do today to leave a lasting impact on the organization tomorrow? ■





Right Size for Success?

By CW3 Zachary Hofstra, 782d MI BN (Cyber), 103 CMT Analysis and Production Chief

Cyber has found success by using the same few people to achieve all of the "wins." This is a function of throwing people at a problem, rather than identifying real work role requirements and then conducting the training and After Action Review required to improve.

The TDA has two SIGINT (Signals Intelligence) Technicians per CMT(Combat Mission Team), commensurate with the size of the SIGINT cell in a Division G2. This roughly matches the levels of responsibility and the size of the adversary or terrain we are expected to perform intelligence on. If we find the adversary or the scope of the mission too outsized from what a Division would take on, that is the sign to request additional intelligence assets, additional time, or a different mission.

Beyond the mission, 780th Military Intelligence Brigade (Cyber) SIGINT technicians are also work role curators, report releasers, planners, Intelligence Oversight Officers, access sponsors, and even assume the role of company commander periodically. These other function steal time from the SIGINT technician's primary function.

Technical knowledge of the target, adversary, and SIGINT systems is critical to becoming a SIGINT Tech; however, understanding Cyber policy and processes make that technician successful on a CMT or CST (Combat Support team). A 352N should hold certifications in three work roles at varying proficiencies: Target Digital Network Analyst (TDNA), Target Analyst Reporter (TAR), Digital Network Exploitation Analyst (DNEA). Outside of the 780th, Soldiers would call all three work roles "SIGINT."

The senior SIGINT technician on a given team is generally the senior intelligence officer and needs to take responsibility for all intelligence functions. Thus, a 780th 352N should manage the other "INTs" Technicians including the All-Source Analyst and the Language Analyst. This responsibility should include the Intelligence Preparation of the Battlefield, the collection matrices/ Intelligence, Surveillance, and Reconnaissance Sync matrix, intelligence oversight, analysis, and reporting. Beyond team responsibilities, SIGINT technicians need to build automated pathways to success. Requirements should include building better exercises, JQRs, and training pipelines. Further, instructing and evaluating should exist within the job description.

Finally, as the senior intelligence personnel, we need to help the cyber community define its intelligence requirements. How many of each work role should a CMT require as a baseline? What is the requirement that drives that number; what is the expectation of the number of reports or operations per week? What metrics should we use? How many TDNAs for a particular problem type; how many DNEAs for a different problem type? Answers to these questions will help leaders better employ our teams on better, more relevant missions. In the end, we need to describe ourselves as a military capability with defined parameters and outputs.

The Australian government describes a military capability as "the combination of force structure and force preparedness." Our CMT/CST structure isn't likely to change drastically, so our preparedness must. We need more and better training, we need TTPs (tactics, techniques, and procedures) and best practices for common problems. We need our battle drill 1A. Steps to team success and individual competencies should be so pervasively understood that failing takes more effort than success.

Our job as warrants is to describe this military capability, provide common training and baselines across the unit, evaluate performance against the baseline, and codify. All of this happens while regular mission never slows down, oversight is a daily requirement, and reports are always in draft awaiting review. The SIGINT CW2 on the TDA can continue to run the day-to-day mission, while the senior SIGINT Tech looks over the horizon and builds the processes to spread success. There is too much work on any given team for just one technician. ■


U.S. AIR FORCE
THE NATION

Making the Cyber School a Viable Assignment for Warrant Officers

By CW4 Todd White, Cyber Training Battalion, Course Manager

Part 1: Manning

THE U.S. ARMY CYBER SCHOOL (AKA, THE "SCHOOL HOUSE") will turn eight years old on August 4, 2022. In those short eight years, it has accomplished some significant strides in advancing Cyber and Electronic Warfare training and providing "the Army with a highly skilled, agile, and innovative Cyber workforce" as its mission statement declares. But these strides were born on the backs of individual effort and not part of a larger strategy. Today, it still struggles to meet the needs of the force with relevant training. The School House faces significant challenges to meet its mandate, prime among these are considerable manning shortages, a conflicted culture, and persistent funding shortfalls. This first part of a three-part article describes these main challenges and possible solutions to mitigate them.

The above table highlights the problem. Of the 20 required instructor positions, based on course length and instructor hours, only 13 are authorized and of these only 11 are filled. With one a known loss and one aligned to efforts outside the Warrant Officer courses, the true number becomes 9. So, the School House is left with less than half the instructors it needs to conduct its courses. Unfortunately, simply a numbers game with assigned personnel doesn't capture the true problem. The amount of time each instructor must spend instructing (or "on podium") is significant, especially when considering that instructors are split between several different MOSs and courses.

Challenge (Manning):

Manning is often the largest challenge discussed amongst leaders and the Warrant School House. On the surface, at a quick glance, the School House might look like it's healthy (as of this writing, it's probably the healthiest it's ever been with two new arrivals); 11 of 13 instructor positions are filled. But the devil is in the details and there are some broken processes behind the School House's manning processes.

	GRADE	POSCO	REQ STR	AUTH STR	POS TITLE	MOS	Rank	Name
170A WOBC	W4	170A8	1	1	SR INSTR	170A	CW4	Filled
	W4	170A8	1	1	INSTR	170A	CW2	Filled
	W4	170A8	1	1	INSTR	170A	CW3	Filled
	W4	170A8	1	1	INSTR			VACANT
	W4	170A8	1	0	INSTR			Not Authorized
17C AIT	W4	170A8	1	1	SR INSTR	170B	CW3	Filled
	W4	170A8	1	1	SR INSTR	170B	CW3	Filled
MSN CDR	W3	170A8	1	0	INSTR			Not Authorized
	W3	170A8	1	0	INSTR			Not Authorized
170A WOAC	W4	170A8	1	1	INSTR	170A	CW4	Known Loss
	W4	170A8	1	1	INSTR	170A	CW4	Filled
	W4	170A8	1	0	INSTR			Not Authorized
	W3	170A8	0	0	INSTR			Not Required in FY23
	W3	170A8	0	0	INSTR			Not Required in FY23
MSN CDR	W3	170A8	1	0	INSTR			Not Authorized
	W3	170A8	1	0	INSTR			Not Authorized
170D WOBC	W4	170D8	1	1	INSTR	170D	CW2	Filled
	W4	170D8	1	1	INSTR			VACANT
WOILE	W4	170A8	1	1	INSTR	170A	CW4	Filled
170B WOBC / WOAC	W4	25S50	1	1	SIGNAL TECH	25S5	CW3	Filled
	W3	170B8	1	1	INSTR	170B	CW3	Filled
	W3	170B8	1	0	INSTR			Not Authorized
			20	13				Total filled: 11

The above table highlights the problem. Of the 20 required instructor positions, based on course length and instructor hours, only 13 are authorized and of these only 11 are filled. With one a known loss and one aligned to efforts outside the Warrant Officer courses, the true number becomes 9. So, the School House is left with less than half the instructors it needs to conduct its courses. Unfortunately, simply a numbers game with assigned personnel doesn't capture the true problem. The amount of time each instructor must spend instructing (or "on podium") is significant, especially when considering that instructors are split between several different MOSs and courses.

The table below displays the relevant Warrant Officer course lengths, total iterations and total weeks per year, along with the authorized versus on-hand instructors, and finally the number of weeks each instructor would notionally be responsible for throughout the year. As noted, with a full complement of 170A instructors, the course load stays manageable. As it stands, one instructor typically assumes the Small Group Leader (SGL) duties for a specific class, handles all the coordination and stays with that specific class as much as possible. Even in this model, instructors from other parts of the School House must be leveraged to teach specific modules within the courses due to requisite expertise. But that's when manning is at 100 percent. As it stands, currently the 30 weeks per year model isn't truly sustainable. Considering there are only roughly 36 weeks of training time in a

Course	Length (weeks)	Classes per year	Total Weeks	Instructors (Auth/OH)	Weeks/ Instructor
170A WOBC	20	3	60	4/2*	15/30
170A WOAC	16	2	32	2/1**	16/30
170B WOBC/WOAC	23	2	46	1/3***	46/15.3
255/170 WOILE-FO	5	4	20	1/1	20

* one WOBC instructor aligned to JCL and functional courses, not part of WOBC cadre

** one WOAC instructor is a known loss with no current projected backfill

*** two 170A instructor billets were advertised as 170Bs to allow for more EW instruct

year, this would leave instructors only six weeks to take their 30 days of authorized leave a year, handle medical appointments, and any other personal issues. This would rapidly fatigue instructors and make the School House an undesirable assignment option.

For 170B instructors, the challenge is more acute. With only one authorized instructor, the course load is impossible. Fortunately, the Senior Warrant Officers in the school house and Office Chief of Cyber recoded two 170A instructor positions as 170B temporarily during a previous movement cycle to allow two additional 170Bs to join the instructor team. This is only a temporary measure as these positions cannot simply be turned into 170B positions as the Cyber School TDA is still governed by TRADOC instructor hours calculations. A great example of this broken process is that from 2020-2021 the 170B course throughput requirements doubled. The Army needed more 170Bs trained. One would think this would result in more instructors. Not so! The doubled throughput resulted in an instructor calculation of 1.95 and TRADOC rounds down. So, no increase in authorized instructors despite the increase in training weeks. This is "doing more with less" exemplified.

This is the broken process that currently exists. The simple mathematical equation is done, but there is no follow up analysis to see if the result is even feasible. It's not just that one person cannot manage 46 weeks of training, that 46 weeks is four separate courses that run independently and often overlap. Without additional support or realistic manning requirements, the result is mission failure.

170D courses were not considered in this article because the courses have yet to complete their pilot phase although one instructor is on hand. Also, sheer length of the 170D WOBC (72 weeks) requires a civilian or contract solution as there likely won't be enough 170D personnel in the Army to begin to meet the instruction requirements.

So far, I have only touched on the simple manning requirements just to conduct Warrant Officer courses in the School House. However, on platform instruction is only half of the instructor's job. All billets are actually "instructor/writer" positions with the expectation that the instructors are spending their off podium/platform time evaluating, updating, and creating new content for the courses. But, if the instructor is spending 30 weeks or more instructing, where is the time to update or create new content? It doesn't exist. Instructors are typically working 11-12 hour days and with so much training to manage, what typically happens is new courseware ideas are captured in random notes and files and then revisited as classes shut down for holiday block leave. Then there is some hasty planning and some more crunching to create new content for the various modules in a race to finish before people head off for leave and holiday travel. And creating new content includes conducting analysis of alternatives, researching costs, coordinating with outside agencies and industry to coordinate training, developing Statements of Work to communicate requirements for vendors. Again, not a sustainable model. If Warrant Officers aren't being employed as course writers and training developers, then Warrant Officers aren't needed as instructors. A contractor can easily deliver course content that never changes.

Finally, another manning challenge facing instructors is the constantly evolving nature of our career field and operational domain. The technology and actors within the Cyber Domain are not defined by the Army or the Joint Force. Each evolves rapidly, often with little notice and requires constant engagement and research to stay apprised of the latest techniques. To keep courseware "relevant" is something of a holy grail quest and trying to address the variety of topics to achieve a common baseline is a significant challenge. Take the 170A WOBC, for example. The goal is to produce a Warrant Officer that is ready to tackle the myriad missions they could face regardless of the formation they find themselves in. In today's force, an individual could pick any one of these topics to dive into and become an expert on, so to find one person to serve as instructor that is an expert in all these varied topics is impossible. "Throwing people at the problem" is not a solution. It must be "throwing the right people at the problem".

Manning (Solutions):

So, we've established that the School House needs more instructors, instructors that have the time needed to develop new content or update existing content, and possess expertise in a wide variety of topics. The School House has attempted to leverage experts from the local operational force units to present course content as "guest instructors." The issue here is that this guest (or adjunct) instruction is all achieved through handshake deals and personal relationships. Teaching a block of instruction in the School House is not the owning unit's priority and can quickly be canceled at the last minute to address any mission requirements. Also, this only addresses the technical expertise and operational relevance of the instruction, it doesn't absolve the assigned School House instructors from being in the room because student to instructor interaction requires specific training and must be monitored. So, a certified School House instructor must be in the room with any guests.

Also, a simple manning update isn't sufficient as the Department of the Army has not authorized seven positions from the TDA. The unit can't simply add seven more requirements to their TDA and hope those will be authorized.

One possible solution to this problem posited by the 780th Military Intelligence Brigade's Senior Technical Advisor, CW4 Erin Ward, involves a plan similar to the guest/adjunct instructor solution but to make it official and part of an individual's assignment lifecycle while at future Fort Eisenhower (the future name of Fort Gordon). Warrant Officers from the operational force would be attached to the Cyber Training Battalion, attend standard instructor training and be aligned to a specific block of instruction for a predetermined time. This would all be captured in the DA 4187 attaching the guest instructor to the School House. They would also be "untouchable" by the

owning unit for the time specified. Ideally, this would be on a volunteer basis but could eventually be mandated or expected and some vetting with the School House instructors would need to occur.

This would also allow the assigned permanent school instructors to move into a more managerial role and truly focus on the writing portion of their duties. This would create an environment where courses could be updated much faster, perhaps even from class to class based on student feedback. This effort would need to be supported by the various commands and captured in a foundational agreement, a Memorandum of Agreement for example, that would mandate each unit's compliance and set the standards for how they support the effort.

In a force that is becoming more stationary and where the Army seems happy not forcing everyone to move every 2-4 years, anyone who wants to do "whatever they can to stay in Georgia" should expect to spend a significant part of their time in Georgia working in the School House. In one's Cyber career, you can pick your job, or you can pick your location. If you want to do a specific job, you go where that job is and plan to move around to get more exposure to diverse mission sets and allow others in the same job to follow you and grow. But, if you're more concerned about where you're working, you don't get to pick every job you do. Doing one job in one place can result in stagnation (some may argue it also results in expertise, but I argue back that it results in very narrow, niche expertise). Only through exposure to a variety of environments do you truly become prepared to defeat a variety of challenges. This a totally feasible solution to, at least, the 170A manning challenges in the School House. But, perhaps, this can reduce the need of 170A instructor positions, and some can be bill payers for additional instructors for the 170Bs. ■

The Enterprise

By CW5 Travis Ysen, Chief Warrant Officer of the Branch

FROM 2015 – 2018, THE CYBER/EW SCHOOl completed a series of initiatives to transition Army Electromagnetic Warfare (EW) from the Fires Center of Excellence to the Cyber Center of Excellence. While the physical and administrative work to accomplish this task was significant, a larger underlying effort is still underway to improve the technical depth and capability of EW personnel and systems. I won't cover all the details of each layer of this multifaceted effort, only a few key points to meet the intent of this particular article.

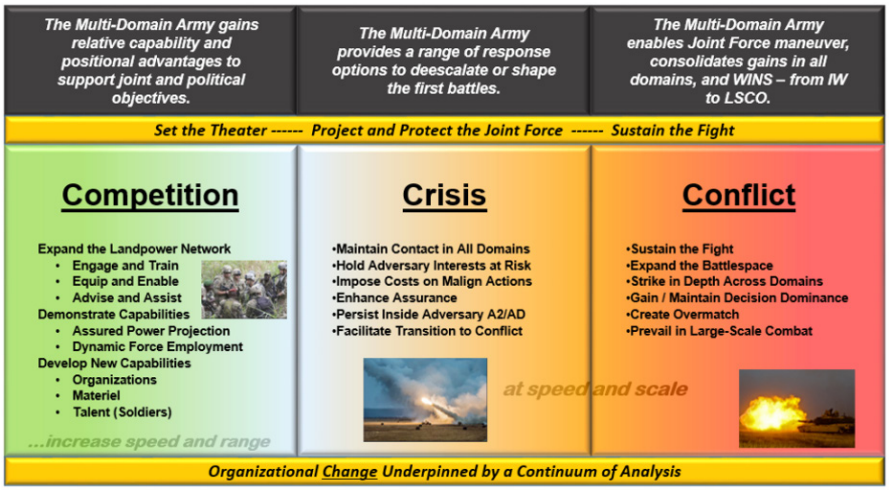


Figure1: Army Multi-Domain Transformation (16 Mar 2021)

During the period that EW was under the Fires branch, there was heavy focus on counter-improvised explosive device (CIED) missions and non-kinetic fires planning. While these very important mission sets were essential to combating the IED threats throughout Afghanistan and Iraq, the technical abilities of the EW cohort within Electromagnetic Support and Attack functions atrophied. This was due to the no-fail nature of the CIED mission; Commanders had to protect people and equipment, which demanded very little risk tolerance regarding EW system setup and employment. So, much of the technical detail in how an EA technique worked and the type of input an EW operator provided was minimized to prevent introducing errors into the systems which may have resulted in loss of life and/or equipment. While the CIED mission remains relevant today, the Army has shifted its focus from counterinsurgency to multi-domain and large-scale combat operations (COIN, MDO, and LSCO), which introduce the concept of competition as being a near steady state with crisis and conflict being aperiodic events. In MDO and LSCO scenarios, our personnel and systems need to be highly capable and responsive to a wide range of threats that leverage the electromagnetic spectrum for communications, system control, and weapons delivery. A cursory analysis of the crisis in Ukraine is a quick validation of this reality.

To highlight the breadth of EW, it is important to lightly review the divisions that form EW operations:

- Electromagnetic Support (ES): the search, detection, intercept, identification, and locating of threat and non-threat emitters in the electromagnetic spectrum (EMS)
- Electromagnetic Protection (EP): actions taken to protect personnel, facilities, and equipment from any effects of friendly or enemy use of the EMS that degrade, neutralize, or destroy friendly combat capability
- Electromagnetic Attack (EA): the use of electromagnetic energy, directed energy, or anti-radiation weapons to attack personnel, facilities, or equipment with the intent of degrading, neutralizing, or destroying enemy combat capability

ES is the foundational component of the EW mission as the Commander's eyes and ears within the EMS. Detection, identification, and location of threats through ES is a primary means of providing combat information that informs protective and offensive measures. Without an EW operator being well versed in emitter detection techniques, EMS search/survey strategies, and emitter knowledge, potential mission failure is extremely high. Therefore, EW operators must be trained to rapidly identify and differentiate threat from non-threat emitters, locate threat emitters on the battlefield using direction finding, geolocation, and dead reckoning techniques, and able to quickly ingest and evaluate combat information for follow-on actions, targeting, and dissemination to the Commander for decision making.

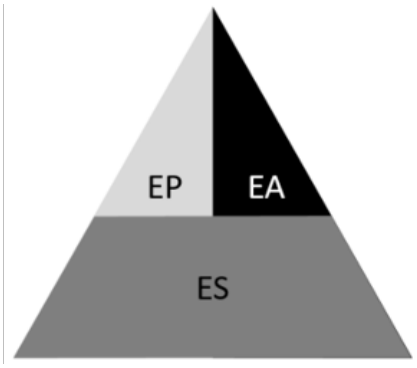


Figure 2: EW Div. of Effort

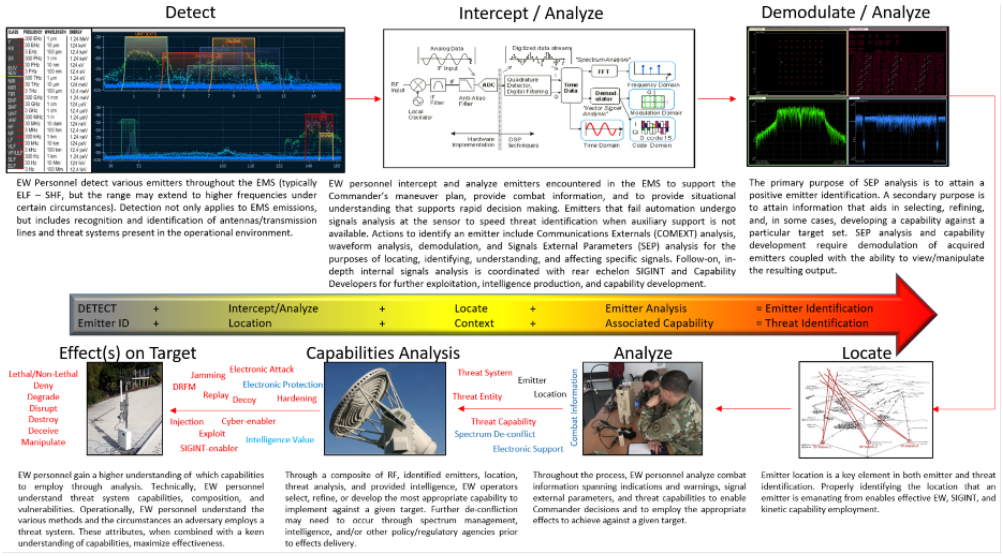


Figure 3: Scope of ES and EA Functions

On the surface, the functions outlined in figure 3 appear to be straightforward. However, EW operators were hampered by overly restrictive policy that prevented them from executing the necessary analytic steps to properly identify emitters and to differentiate emitters that employ similar modulation and transmission modes. As the EMS becomes more congested, the ability to perform analysis is critical, even more so when operating in a contested environment where adversarial EA techniques may be less obvious than traditional noise jamming of the past.

Work to adjust policy began in earnest in 2017 with direct engagements with the Army Cryptologic Office, NSA's Electromagnetic Warfare Office, the Army G2, Army Cyber, and select EW professionals from across the operational force. The goal was to enable EW personnel to demodulate and analyze the resulting signal structures when automation failed to provide an emitter identification. The initial positive step to an accepted and implemented policy change was with the publication of Army Directive 2019-22, signed on 27 June2019. This directive identified ES as a shared task between EW and SIGINT missions and that demodulation and signals external parameter analysis, which includes signal structures, were authorized EW operator activities. While this was a significant step in the right direction to empower and enable our EW cohort, the directive is only an interim solution until these activities are written into Army regulation. Shortly after the directive was published, work to develop an updated EW Army regulation (AR 525-24) began. The original publication was projected for June of 2021. However due to several challenges primarily linked to the pandemic, progress was extremely slow. Recently, the draft AR passed through its first legal review, was updated by HQDA EW personnel, then shared with the Principal Cyber Advisor to the Secretary of the Army and Chief of Staff of the Army for additional review. Based on this progress, publication may be forthcoming within FY23.

In 2020, a secondary effort called STARBLAZOR was initiated to identify and resolve methods for Army Cyber to detect, intercept, sample an emitter, then rapidly develop and deliver an electromagnetic countermeasure (ECM) for operational employment. The 915th Cyber Warfare Battalion was the primary unit involved in executing the functional portions of the process with the Cyber Solutions Detachment providing ECM development support. Additional support was provided by ARCYBER, the CCOE, PEO IEW&S, Intelligence Center of Excellence (ICoE), Headquarters, Department of the Army (HQDA) Assistant Deputy Chief of Staff for Department of the Army's Management Office-Strategic Operations (DAMO-SO), Army Reprogramming Analysis Team-Program Office (ARAT-PO), Command, Control, Communications, Computers, Combat Systems, Intelligence, Surveillance and Reconnaissance (C5ISR), Intelligence and Security Command (INSCOM), and Army Cryptologic Office (ACO) which speaks to the importance of this initiative. The 915th successfully executed the process against a target emitter in a live environment in the summer of 2021, validating that the concept had potential to change how radio reprogramming occurred in the past.

While the initial STARBLAZOR pilot was a successful demonstration of an alternative rapid ECM development and delivery process, additional work is needed to include SIGINT functions. Studies associated with the pilot identified 17E/170B, 17D/170D, and 35S/352S core competencies, as well as produced a task crosswalk to help identify overlap and distinction areas. However, employment of SIGINT personnel and processes was not included in the study. Despite this, the information was key to understanding of how these MOSs could work together for ECM development. It also helps inform other efforts to integrate EW and SIGINT missions on the battlefield.

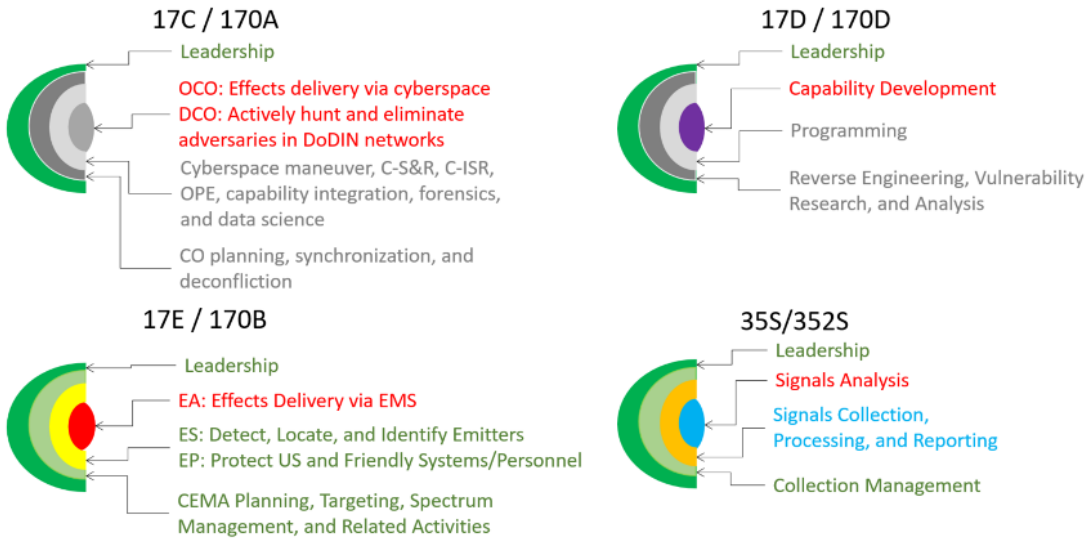


Figure 4: MOS Core Competencies (Jawbreaker view)

Taking a close look at the core competencies of each MOS considered during the STARBLAZOR study provided better insight into their specific functions across a range of scenarios. For the purposes of this particular portion of the study, a central core competency was defined as a unique function that the Army requires of the MOS that no other MOS provides. Looking at the very core of an MOS should reveal a singular task. However, an MOS like 170A reveals a split core traversing both OCO and DCO competencies (another topic altoghether). Competency layers beyond the central core are secondary and tertiary competencies. For instance, a 17E/170B's central core competency is, "EA: Effects Delivery via EMS" with secondary competencies being ES and EP and CEMA activities being tertiary competencies. The idea is that secondary and tertiary competencies may be tasks that other MOSs also provide. For example, while not labeled as such, with ES having been identified as a shared or common task between EW and SIGINT, would show up as subtask within 35S/352S's, "Signals Collection, Processing, and Reporting" secondary layer.

Beyond classifying unique and similar competencies, further consideration of how these MOSs complement each other is required. What I lightly call, "The TRIFECTA of Pain" is an idealization of three functional areas (EW/SIGINT/Cyber) working together in concert to rapidly identify, reverse engineer, and develop capabilities that support operational requirements in an efficient and effective manner. 17E/170B serve as the execution arm for effects delivery in and through the EMS, 35S/352S provide signals analysis support to the EW operations as well as capability development, and 17D/170D work with both entities to develop and deliver capabilities that are relevant and on time.

To expand this concept, consider the processes depicted in figures 6 and 7. 17E/170B may also provide support to the rapid capability development process (capabilities that may not require a high degree of sophistication) by providing signal external parameter analysis results to the 17D/170Ds. 17E/170B may also inform 35S/352S signals analysis emphasis by providing information that filters out signals of interest from the chaff; enabling the 35S/352S to focus on new and unusual signals. Both 17E/170B and 35S/352S may support the Commander's Critical Information Requirements through combat information and/or actionable intelligence. The 35S/352S may have an additional, but complimentary task of supporting specific intelligence requirements.

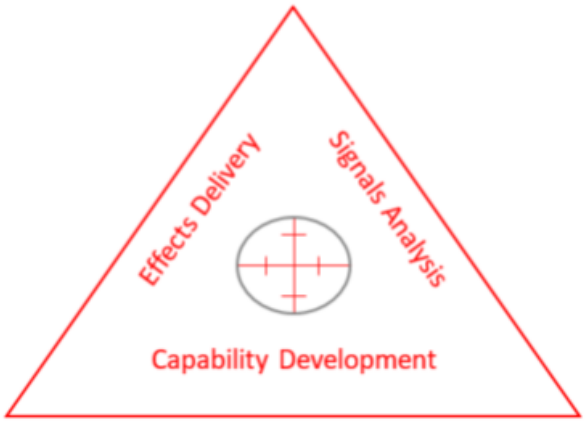


Figure 5: TRIFECTA

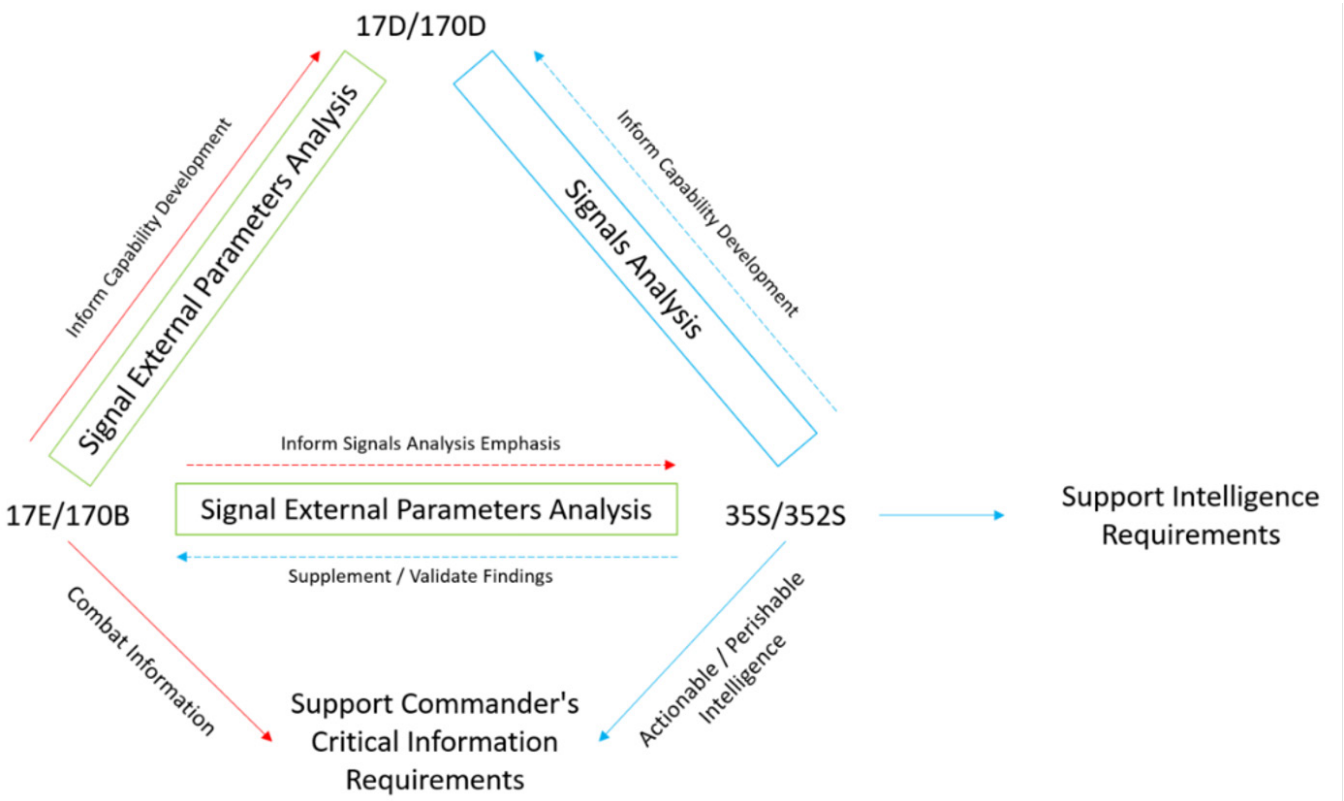


Figure 6: MOS Focal Points

In October, 2021, United States Signals Intelligence Directive (USSID) 305 was updated. This provides a process for non-SIGINT entities to attain approval to employ SIGINT equipment under certain circumstances. The non-SIGINT entities are required to submit a request to use SIGINT equipment and must meet SIGINT training, compliance and oversight requirements. While USSID 305 supports EW personnel operating SIGINT equipment that may be more capable than traditional EW systems, EW systems need to be designed to support authorized activities (demodulation and signal external parameter analysis). This would enable USSID 305 to serve as a supplemental method to increase capability for specific missions rather than a mainstay for routine operations. The purpose of EW personnel conducting demodulation and signal external parameter analysis is not to conduct SIGINT or to take over 35S/352S roles, but to provide a more seamless effort between the MOSs. A well trained EW operator capable of performing adequate analysis of a specific emitter saves countless 35S/352S man hours by providing accurate samples of emitters that truly require signals analysis. While serving as a 352S, I personally experienced the challenge of having a poorly trained collector workforce provide a multitude of non-important data samples due to them not exercising good emitter identification practices which requires demodulation and signals external parameter analysis.

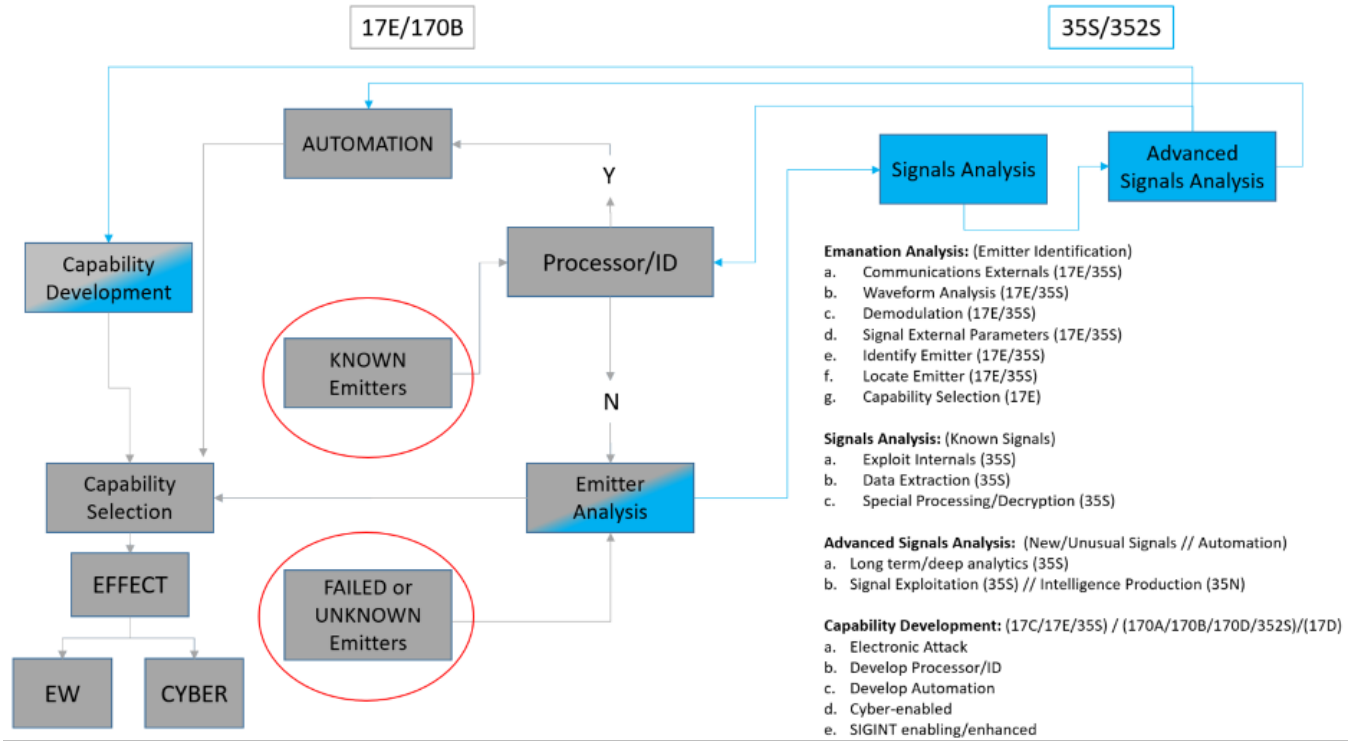


Figure 7: MOS Cooperative Effort

A lot of necessary time and energy has been spent rendering out MOS and mission differences. It's time we start looking more seriously at what EW/SIGINT/Cyber integration means and how to do it efficiently and effectively. I think we can avoid unnecessary duplication of effort and misaligned functions by considering core competencies as a foundational component of employment strategies. This leads to the title of this particular article, "The Enterprise." I've laid out a few thoughts on how I think a segment of our EW/SIGINT/Cyber MOSs could work together in a larger construct. However, as somewhat of a singular viewpoint, added input from the team would be useful in formulating a good way ahead that places the Army in an advantageous position to optimally leverage the skills and abilities of its personnel. Having navigated through much of the processes and systems to get to where we are today, the enterprise exists… we just need to bring it together to make it work for us and not against us!

Figure 8: NTC_Tiefort_Mtn_CW3_Strickland_CW5_Ysen_COL_Holland_COL_Salas

Quiet Pro

ofessionals

How Will USCYBERCOM's Past be Present in its Future?

By CW3 Justin Helphenstine and CW5 James Richards

Introduction

CHARLES DICKENS INTRODUCES EBENEZER SCROOGE as a man awash with resources but with an impoverished soul. Visited by his former business partner, Scrooge learns he wears invisible chains, forged link by link at each juncture where he chooses wealth for wealth's sake. Over the course of an enchanted evening, Scrooge receives three spirits – of past, present, and future, who grant him the outsider's view of his own life. These spirits lead Scrooge to recognize a sense of purpose and a corresponding need for change to align with that purpose. Ebenezer awakes, wiser for having examined his life, and proceeds to fight for an altered future.

This allegory serves U.S. Cyber Command well. Over a decade after its birth, the Command has all the elements – a business partner with its own lessons learned, a past and present silhouetting the future's path, and opportunities to alter course. USCYBERCOM wears different chains, forged instead by metrics grounded in Measures of Performance (MOPs), constraining the Command's vision for itself. How might USCYBERCOM's nighttime visit play out if it were visited by its own ghosts? How might the command be moved to second performance to effectiveness?

Data, the Ghost of Cyber Past

Data inherently tells the story of the past. The first ghost would point to the Command's early and ongoing recognition of the need to organize and employ its data, both with systems like Unified Platform as well as major acquisition programs like the Joint Cyber Warfighting Architecture, holding a vision for how data will be handled as a commodity. These aspirations mask a Command with a nascent lexicon and no single data model governing operations. This deficit deprives the Command of data-driven decision-making; instead of continuous, accurate data, decisions are at best informed by expensive data calls with forage for relevant data, some of which begins expiring the moment it is observed.

USCYBERCOM should be at the forefront of alloying Defensive Cyberspace Operations (DCO) and Offensive Cyberspace Operations (OCO) data into a unified model of blue and red activity, and data standards are essential to realizing that opportunity. It's important to obtain those future data management systems, but think of them as refineries, with efficiency constrained by the quality of the inputs. USCYBERCOM gets to "make" its own ore; is that a decision best left fragmented across independent actors, or unified across the community as the ghost implies?

Delegation, the Ghost of Cyber Present

Continuing the journey, USCYBERCOM might conclude the next ghost, Delegation, makes for a victory lap. USCYBERCOM is on the cusp of delegating OCO authorities to Subordinate Headquarters (Sub-HQ) Commanders. Adoption of the Operations Risk Management Framework in 2021 set the stage for this delegation; the ghost would faithfully show the Sub-HQs preparing the local policies and establishing the workflows enabling them to wield these delegated authorities. But far from the Sub-HQs, at the tactical edge, other units would clamor for attention; units such as the US Marine Corps' Cyberspace Mission Elements (CMEs), US Army Expeditionary Cyberspace Teams (ECTs), or the US Army National Guard's Cyberspace Warfare Companies (CWCs).

The ghost would point out that while delegation is poised to empower the Sub-HQs, these tactical outliers aren't postured to reap the benefits of moving at the speed of trust. Their irregular nature and emerging operational concepts require handling multiple authorities, blending non-OCO authorities with OCO ones, and normalization of their mission space in both mission and capabilities management processes. Unencumbered by managing affairs soon left to the Sub-HQs, USCYBERCOM should pivot staff resources to legitimize and empower the tactical edge, ensuring their presentation to Unified Combatant Commanders is more than PowerPoint-deep.

Dependence, the Ghost of Cyber Future

USCYBERCOM's future is firmly grounded in its past affiliation with the National Security Agency, and nowhere is this more constraining than in how the Command measures itself. This ghost would show a not-so-distant future where USCYBERCOM continues to elect to measure the readiness of its forces by a Combat Support Agency's yardstick, structurally embedding an inferiority complex and abrogating its responsibility to set joint training standards. The ghost of the future would also likely show shadows of a Command continually dependent on the NSA, not as a peer organization, or as a Unified Combatant Command partnering closely with a Combat Support Agency. In such a future, USCYBERCOM continues forging its chains, notching Measures of Performance indexed to intelligence work.

Measurement is a powerful tool, though, and Peter Drucker wisely observed "What gets measured gets managed." The Command could chart a different course, but it begins with answering questions at the core of its identity: What are USCYBERCOM's deliverables? A starting point might be coverage of Combatant Commanders' priorities with offensive kill chains; seeking to raise this number could in turn drive capability coverage of essential technologies, or development

and maintenance of certain tradecraft. The currency of any such kill chain would drive measurements of rehearsals, in contrast to simply counting operations. The utility of intelligence furnished by the NSA in supporting answering these questions offers a measure of effectiveness in evaluating the partnership between Command and Agency. These proposed reforms in metrics offer an alternative future, one where the Command's understanding of itself matures alongside its relationship with the NSA; a future building on the past, but not bound by it.

Conclusion

USCYBERCOM's future is brighter than ever. The ever-matriculating talent pool within the Command grows its collective knowledge, and while individuals rotate in and out, the aggregate maturity of the Command is not in doubt. What the shades of past, present, and future presented above show is the Command's control of its trajectory – from gradual, grinding rise as measured by Measures of Performance, to rapidly becoming the preferred partner of Combatant Commanders and National decision-makers for Cyberspace Operations as measured by outcomes. The former will likely see the Command seconded in the halls of power to other organs of state; the latter postures the Command for further investment. The status quo sets the stage for friction with the Service Components who sincerely want to experiment with, develop, and present tactical cyber elements; the brighter future forges trust at echelon with USCYBERCOM facilitating the Services' natural relationships with other Combatant Commanders, as well as their role in building forces.

Ebenezer wakes up answering the call to action, determined to mend his ways. A personified USCYBERCOM might awake from such a night in a Joint Mission Operations Center, looking around at the previously invisible chains now plainly holding it down and resolve to do the same. Through its future data management systems, delegation, and evolving style of OCO, the Command is already transforming itself for the better and moving away from forging more links in those chains. As both Ebenezer's and USCYBERCOM's nighttime sojourns show, though, there's plenty of room left for improvement. Past may be a prologue, but it needn't be a prophecy. ■

FORT GEORGE G. MEADE, Md. -- U.S. Cyber Command, Cyber National Mission Force members participate in a training and readiness exercise at Fort George G. Meade, Md., May 24, 2021. The CNMF plans, directs and synchronizes full-spectrum cyberspace operations to disrupt, degrade and defeat malicious cyber actors. (photo by Josef Cole, U.S. Cyber Command)

Warrant Officer – Master Shammer or Dedicated Technician? Yes.

By CW2 Steve McCoy, 782d MI BN (Cyber), 102 CMT

THE OFFICIAL BIRTHDAY OF THE ARMY WARRANT OFFICER is July 9, 1918, when an act of congress established the Army Mine Planter Service as part of the Coast Artillery Corps, replacing an informal service crewed by civilians with military personnel. However, the Warrant Officer's lineage can also be traced to 1896 with the War Department's creation of civilian Headquarters Clerks and Pay Clerks. Following many years of specialized work, these civilian clerks would become official military members, initially considered enlisted Soldiers but eventually being recognized as Army Warrant Officers.

Army Warrant Officers make up the technical foundation of the U.S. Army. They possess a high degree of specialization in a particular field in contrast to the more general assignment pattern of other commissioned officers. They are highly trained technical experts who specialize in one of 47 technical areas including cyber warfare, intelligence, field artillery, and aviation. Although making up less than three percent of total Army strength, Warrant Officers serve as the technical experts and trusted advisors to commanders at all echelons. Warrant Officers are expected to constantly perform with high levels of precision and aptitude to administer, manage, maintain, operate, and integrate Army systems and equipment across the full spectrum of operations.

Throughout the past century, a great number of Warrant Officers have served within the U.S. Army, providing commanders with a unique skillset acquired over many years of experience. While traditionally performing primarily technical duties, the Army Warrant Officer is also a well-trained and focused combat leader. Warrant Officers are adaptable and agile professionals, able to excel in not only their area of expertise, but in any environment in which they operate. Warrant Officers have performed many of the military's most celebrated and prestigious tasks, both technical and tactical, solidifying their reputation as versatile problem-solvers.

We all know about the great heroism the master tactician known as Warrant Officer Flint (top), of Chief Michael Durant (middle) as the pilot of Super Six Four during Operation Gothic Serpent, and Chief Roy Miller (bottom) desperately searching for WMDs in the 2010 action-thriller blockbuster Green Zone, but this article aims to provide a brief glimpse into some of the lesser-known contributions of the Warrant Officer Cohort.

Thomas J. Hennen
The first Warrant Officer within the Department of Defense selected as a member of a Space Shuttle flight crew

After enlisting in 1973, Chief Hennen served over 23 years in the imagery intelligence field. He received extensive technical training and experience as an operational imagery analyst at both the national and tactical levels; experience as an instructor; training, force, and combat developer; extensive material development and acquisition management experience - all of which combined to make him one of the most qualified imagery intelligence technicians within the Department of Defense (DOD).

In 1986, Hennen was selected by the Commanding General of the U.S. Army Intelligence Center to represent him within the U.S. Army Space Program Office in Washington, D.C., for those matters pertaining to Tactical Exploitation of National Space Capabilities Program (TENCAP) requirements, concept development, and the doctrinal and operational employment of TENCAP systems. Additionally, he was a member of various DA, DOD, and national intelligence community working groups and subcommittees involved in TENCAP program activities.

Chief Hennen was selected as a payload specialist astronaut candidate in September 1988 and began Terra Scout payload operations training at Fort Huachuca, Arizona in March 1989. During August 1989, Tom was selected as the primary payload specialist for the Terra Scout experiment manifested on STS-44. He reported to NASA in 1990 to begin Payload Specialist Astronaut training.

CWO Hennen became the first Warrant Officer in space, flying aboard the Space Shuttle Atlantis (STS-44), which launched from Kennedy Space Center, Pad 39A at 6:44PM (EST), November 24, 1991. He orbited the Earth 109 times, traveling 2.9 million miles, before landing at Edwards Air Force Base, California on December 1, 1991.

Olive Hoskins
The first woman Warrant Officer in the United States Army

Although Olive Hoskins, an Army civilian grade military clerk, was appointed a Warrant Officer in 1926, available records indicate that March 1944 was the date of official initial accessions of women into the Warrant Officer Corps. Before then there existed a question as to whether or not women Soldiers could be appointed Warrant Officers if they held positions which, for a man, carried the grade. Legislation concerning the Women's Army Corps did not mention the matter, and on this basis the Judge Advocate General ruled that appointment of women was illegal because the law did not specify that it was legal. The question was brought to the War Department's attention by several high-ranking officials who wished to appoint the Warrant Officer grade to the women who were filling appropriate positions. The Judge Advocate General was overruled and the Department of the Army G-1 held that such appointment was legal under the general authority to admit women to full army status, with the Chief of Staff upholding this opinion. At the end of World War II, 42 women were in the Warrant Officer Corps.

Not only was Olive the first woman Warrant Officer, but she essentially set the standard for all future Warrants to follow. According to a 1933 newspaper article, throughout her career Olive Hoskins "never [wore] a military uniform, never had to salute a superior, was never awakened by reveille, never slept in a pup tent, and never stood in line for mess." And you thought a backup PC left on your desk was high-level shamming.

Michael J. Novosel

Recipient of the Congressional Medal of Honor for his actions in the Vietnam War

Ok, Ok… I know the introduction to the article primarily focused on Warrant Officers being technical experts. The thing is, Warrants are typically divided into two distinct categories: Technicians and Pilots (or flight Warrants). Now I'm certainly not suggesting flight Warrants are not experts or their job is not technical (they are and it is), I'm simply keeping the text relevant to our environment here in the 780th. However, the actions of Michael Novosel were too important to ignore. This Warrant Officer truly exemplifies the commitment of not only the Cohort, but of the American Soldier. I'll just let his citation do the talking:

Medal of Honor citation:

For conspicuous gallantry and intrepidity in action at the risk of his life above and beyond the call of duty. CWO Novosel, 82d Medical Detachment, distinguished himself while serving as commander of a medical evacuation helicopter. He unhesitatingly maneuvered his helicopter into a heavily fortified and defended enemy training area where a group of wounded Vietnamese Soldiers were pinned down by a large enemy force. Flying without gunship or other cover and exposed to intense machinegun fire, CWO Novosel was able to locate and rescue a wounded Soldier. Since all communications with the beleaguered troops had been lost, he repeatedly circled the battle area, flying at low level under continuous heavy fire, to attract the attention of the scattered friendly troops. This display of courage visibly raised their morale, as they recognized this as a signal to assemble for evacuation. On 6 occasions he and his crew were forced out of the battle area by the intense enemy fire, only to circle and return from another direction to land and extract additional troops. Near the end of the mission, a wounded Soldier was spotted close to an enemy bunker. Fully realizing that he would attract a hail of enemy fire, CWO Novosel nevertheless attempted the extraction by hovering the helicopter backward. As the man was pulled on aboard, enemy automatic weapons opened fire at close range, damaged the aircraft and wounded CWO Novosel. He momentarily lost control of the aircraft, but quickly recovered and departed under the withering enemy fire. In all, 15 extremely hazardous extractions were performed in order to remove wounded personnel. As a direct result of his selfless conduct, the lives of 29 Soldiers were saved. The extraordinary heroism displayed by CWO Novosel was an inspiration to his comrades in arms and reflect great credit on him, his unit, and the U.S. Army.

Ellen Ripley

Warrant Officer aboard the famed freight spacecraft Nostromo

Beginning her career as a warrant officer with Weyland-Yutani Corporation's commercial freight operations, Ripley was assigned to USCSS Nostromo in 2122 when it encountered a single Xenomorph unintentionally collected from the moon Acheron (LV-426). This event led to the death of the rest of Nostromo's crew and the destruction of the ship. Ripley's encounter with the Xenomorph would fundamentally alter the course of her life.

Later promoted to Lieutenant First Class and attached to the Colonial Marines as a civilian adviser, Ripley would go on to have several more encounters with the creatures over the following decades, before eventually sacrificing herself on Fiorina "Fury" 161 to put an end to the Alien menace once and for all. Her exploits ensured that she was well-known among groups and individuals that dealt with the Xenomorph for decades, even centuries, after her death. ■

References:

FM 6-22

The Brooklyn Daily Eagle Brooklyn, New York. 12 Januray 1933

1. https://www.army.mil/medalofhonor/citations26.html

2. https://www.warrantofficerhistory.org/Hist_Women_WO.html

3. https://web.archive.org/web/20101108071015/http://www.history.army.mil/html/moh/vietnam-a-l.html

4..https://www.army.mil/medalofhonor/citations26.html

5 https://www.goarmy.com/careers-and-jobs/current-and-prior-service/advance-your-career/warrant-officer.html

6. https://usacac.army.mil/organizations/cace/wocc/woprogram

7. https://avp.fandom.com/wiki/Ellen_Ripley


U.S. Army
Warrant Officer
Mine Planter Service,
Coast Artillery Corps
Established July 9, 1918

The Honorable Order of Saint Isidore

PRAETORIANS,

The Honorable Order of Saint Isidore is an Armed Forces Communications and Electronics Association award given to individuals who have demonstrated exceptional initiative, leadership, insight, and cyber excellence in their area of expertise. The award is comprised of the Gold, Silver, and Bronze Medallion. The Gold Medallion is for those who have rendered conspicuous long-term service and significant contributions to the cyber mission force. The Silver reflects those with contributions toward the promotion of the cyber mission in ways that stand out in the eyes of the recipients, their superiors, subordinates, and peers. The Bronze medal is for people with the highest standards of integrity, moral character, professional competence, selflessness, while contributing to the betterment of the cyber mission force.

The command team and I would like to congratulate the following 780th MI Brigade personnel for their selection to receive the 2022 Saint Isidore Award.

Gold award:
CW4 Dustin M. Lee, Task Force Echo
CSM Marlene N. Harshman, 915th CWB
CSM Kermit D. Harless, Task Force Echo

Silver award:
LTC Benjamin H. Klimkowski, 915th CWB
CW4 Erin Ward, 780th MI BDE (Cyber)

Bronze award:
CW4 Kathy A. Hall, 782d MI BN (Cyber)
CW4 Kevin A. McKee, 782d MI BN (Cyber)
CW3 Gerald C. Cleven, 781st MI BN (Cyber)
CW3 Christopher D. Shepard, 781st MI BN (Cyber)
1SG Adam T. Brege, 915th CWB
1SG Nicholas J. Davis, 915th CWB
1SG Carlos De La Cruz, 915th CWB

Please take the time to congratulate this year's winners.

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


MILITARY ORDER OF SAINT LOUIS

SLOAN, Nv. - Soldiers from the 780th Military Intelligence Brigade (Cyber) supported a Las Vegas STEM (Science, Technology, Engineering, and Mathematics) Fair – sponsored by the U.S. Army –showcasing STEM-related career fields in the Army and Army Reserve for 49 local schools at the George W. Dunaway U.S. Army Reserve Center, April 6 and 7. The Praetorian 17C, cyberspace operations specialists, designed their own interactive "cyber challenge" (CTF) to encourage student interest. PFC Sanchez, a graduate of Coronado High School, Las Vegas, was at the same STEM event three years ago and talked about his journey from hometown to cyber warrior.

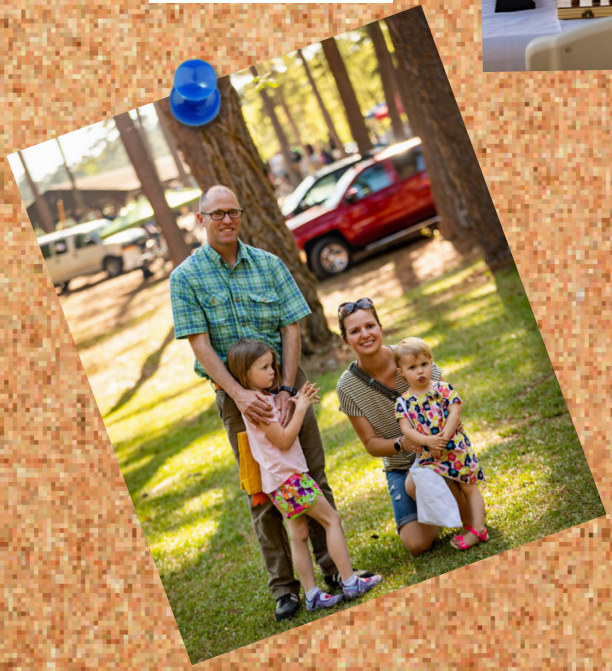
CHICAGO, Il. – Soldiers from the 780th Military Intelligence Brigade (Cyber) supported a job fair at the Chicago Cyber Conference (ChiCyberCon) hosted by the Illinois Institute of Technology (Illinois Tech), in Hermann Hall, April 14. The Soldiers developed a "Cyber Challenge" CTF to encourage the participant's interest. At the end of the day, their table was the last one with people still at it. Great job Praetorians – Telling the Army Story...telling the Army Cyber Story!

FORT GEORGE G. MEADE, Md. – 781st Military Intelligence Battalion (Cyber) Relinquishment of Responsibility whereby Command Sergeant Major Kelly J. Barnes relinquished his responsibility as the battalion senior enlisted leader and 'Keeper of the Colors' in a ceremony hosted by Lieutenant Colonel Michael L. Arner, at the Post Theater, April 15. Immediately following, the battalion and the 780th Military Intelligence Brigade (Cyber) honored CSM Barnes and his Family's service in his retirement ceremony.

FORT GEORGE G. MEADE, Md. – Headquarters and Headquarters Company (Hastati), 780th Military Intelligence Brigade (Cyber) Change of Command ceremony whereby CPT Lauren Feifer relinquished her command to CPT Alvaro Luna in a ceremony hosted by COL Matthew Lennox, the brigade commander, at the MG Baron DeKalb Army Reserve Center, April 15.

FORT GEORGE G. MEADE, Md. – The Soldiers, Army Civilians, Family, and friends of the 780th Military Intelligence Brigade (Cyber) bid a fond farewell to First Sergeant Tammy E. Cross and her Family, during a retirement ceremony hosted by Colonel Nadine K. Nally, at the DeKalb Army Reserve Center, April 22.

FORT GEORGE G. MEADE, Md. – Headquarters & Headquarters Company (Hastati), 780th Military Intelligence Brigade (Cyber) Change of Responsibility whereby First Sergeant Edgar O. Morales relinquished his authority as the senior enlisted leader and “Keeper of the Colors” to 1SG Rafael A. Ortiz in a ceremony hosted by Captain Alvaro A. Luna, at the DeKalb Army Reserve Center, April 22.



APPLING, Ga. – The 782nd Military Intelligence Battalion (Cyber) conducted their annual Spring Festival at Wildwood Park, April 22. The event enabled service members, Civilians, and Families to socialize and build cohesion in a family-centric environment. Several Soldiers were recognized with military awards for their exceptional performance and support to military operations. Cyber Legion families enjoyed quality food, a volleyball tournament, a chess tournament, egg scavenger hunt, inflatable bouncy houses, and several yard games. Bravo Company (Birds of Prey), 782d MI BN, shined in the competitions by winning the volleyball tournament, the chess tournament and earning the battalion leader's PT streamer.

FORT GEORGE G. MEADE, Md. – Command Sgt. Maj. Ronald Krause, 780th Military Intelligence Brigade command sergeant major, presented the Sergeant Audie Murphy Award to Sgt. 1st Class Andrea Collins, 782nd Military Intelligence Battalion senior digital network analyst sergeant for E. Company, during a ceremony at the post theater May 17, 2022.

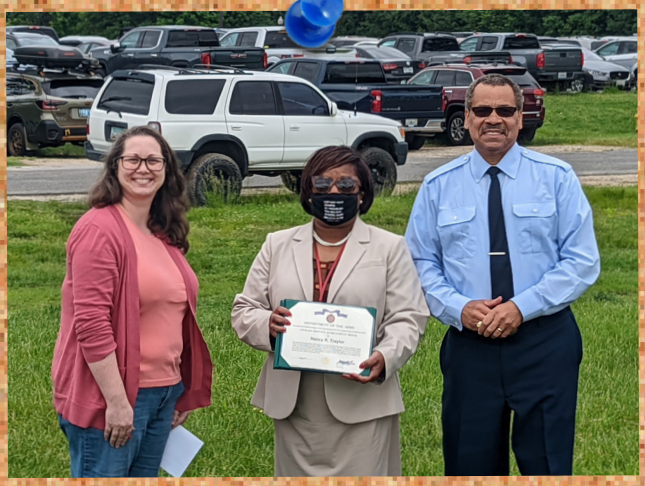
LACKLAND AFB, Tx. – Detachment Texas (Cyber Rangers), 782nd Military Intelligence Battalion (Cyber), Change of Command whereby Lieutenant Colonel Jason H. Seales relinquished his command to Major Matthew D. Heinmiller in a ceremony hosted by LTC Thomas M. Nelson, the battalion commander, in Arnold Hall Community Center, May 25.

FORT GORDON, Ga. – Warrant Officer Nelson (Distinguished Honor Graduate), WO1 Ware (Honor Graduate), Chief Warrant Officer 2 Martin and CW3 Reed, assigned to the 782D Military Intelligence Battalion (Cyber Legion), graduated from the 170A, Warrant Officer Basic Course on June 13.

FORT GEORGE G. MEADE, Md – Congratulations to (from left to right): CPT Neil Marklund, CPT Sean Little, CPT Cullen Acheson, and CPT Michael Nelson, on their promotion to Captain, May 6. The officers are assigned to the 781st Military Intelligence Battalion (Cyber), Vanguard…When Others Cannot.

FORT GEORGE G. MEADE, Md – B Company (Immortals), 781st Military Intelligence Battalion (Cyber), Change of Command whereby Captain Sacarra G. Pusey relinquished her command to CPT Allan A. Baily in a ceremony hosted by Lieutenant Colonel Michael L. Arner, the battalion commander, at the MG Baron DeKalb Army Reserve Center, May 13.

FORT GEORGE G. MEADE, Md. – C Company (Conquerors), 781st Military Intelligence Battalion (Cyber), Change of Command whereby Captain Joseph E. Kim relinquished his command to CPT John M. Cloutier in a ceremony hosted by Lieutenant Colonel Michael L. Arner, the battalion commander, on the Parade Field, May 20.



FORT GEORGE G. MEADE, Md. – Nancy Traylor (center), Deputy Civilian Personnel Officer, 780th Military Intelligence Brigade (Cyber), received the Civilian Service Achievement Medal, Certificate of Achievement, Army Civilian Service Recognition Pin-Bronze, and a Time Off Award, from Katie Jane (left), Civilian Personnel Officer, and Dean Courtney (right), brigade resource manager, on the Brigade soccer field, May 25.

FORT GEORGE G. MEADE, Md. – SPC Gavin Hawthorne (center), Headquarters & Headquarters Company, 780th Military Intelligence Brigade (Cyber), was promoted to Specialist by SGT Nicholas Garzon (left) and 1SG Rafael Ortiz, the company first sergeant, on the Brigade soccer field, May 25.

FORT GEORGE G. MEADE, Md. – Ronette Jarvis (center), S2 section, 780th Military Intelligence Brigade (Cyber), received the Civilian Service Achievement Medal, Certificate of Achievement from CPT Alvaro Luna (left), commander, Headquarters & Headquarters Company, 780th Military Intelligence Brigade (Cyber), and Terrance Perry, Brigade S2, on the Brigade soccer field, May 25.

FORT GEORGE G. MEADE, Md. – Chief Warrant Officer Five James Richards was promoted in front of his fellow Warrant Officers, Soldiers, Family and friends in a ceremony hosted by Colonel Matthew Lennox, commander of the 780th Military Intelligence Brigade (Cyber), at the DeKalb Army Reserve Center, June 10.

FORT GEORGE G. MEADE, Md. – Soldiers and Civilians of the 780th Military Intelligence Brigade (Cyber) recognized the selfless service and sacrifice of Lieutenant Colonel Jesse Sandefer and his Family for more than 22-years of honorable service to his nation in a retirement ceremony at the DeKalb Army Reserve Center, June 10.

FORT GEORGE G. MEADE, Md. – Soldiers and Civilians of the 780th Military Intelligence Brigade say farewell to the Brigade S3 in front of the Brigade Headquarters, June 10.

FORT GORDON, Ga. – 782d Military Intelligence Battalion (Cyber) conducted a Best Squad Competition from June 6 through 9. Squads from Charlie Company (Centurions) and D Company (Dracones) competed in physical, tactical, and technical challenges ranging from squad level warrior tasks to a cyber-capture the flag mystery event. Congratulations to SSG Benjamin Bolin (35P), SGT Nicholas Grant (35P), SPC Nathaniel Mattson (17C), SPC Ian McQueen (17C), and SPC Kolby Stevenson (17C) of D Company, 782d Military Intelligence Battalion (Cyber) on your victory. PRAETORIANS, STRENGTH AND HONOR!

NEXT QUARTER'S BYTE IS focused on the NCO - "the backbone of the Army"- past, present, and future. As in other issues of the BYTE magazine, the command encourages your contribution to drive the Cyber and Information Advantage conversation. If you have an article to share, write a synopsis and send it to steven.p.stover.civ@army.mil NLT August 15, 2022. Final articles are due August 31.