

780th MILITARY INTELLIGENCE BRIGADE (CYBER)

THE BYTE

Vol. 13, Issue 2

April 2025



SUCCEEDING:

As an Army Operating in a Joint Environment



780th MI BDE
"STRENGTH AND HONOR"

COL Candy Boparai
Commander
CSM Joseph Daniel
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@army.mil, or mail to 310 Chamberlin Avenue, Fort George G. Meade, MD 20755, or call (301) 833-6430.



P6 BYTE Introduction COL Candy Boparai, BDE CDR, 780 MI BDE (Cyber)	1
11th Cyber Battalion "Leviathans" <i>"Global Reach, Global Impact!"</i> MAJ Vincent E. Michel, IA Cell Lead, 11th CY BN	3
11th Cyber Battalion supports U.S. Army Rotational Training Units at NTC	4
Army Leadership in a Joint Environment LTC Thomas Schindler, 781st MI BN (CY)	8
Bridging the Divide; Cultivating Success in Joint Military Operations 1LT(P) Stephen Romer, 781st MI BN (CY)	10
Giving Due Credit in a Joint Environment 1LT Matthew Holcomb, 781st MI BN (CY)	12
Vanguard Battalion Relinquishment of Responsibility – Farewell to a Beloved Leader 781st MI Battalion (Cyber)	13
How Combatant Command Cyber Protection Team (C-CPT), 503 CPT, Task Organized to Support Joint DCO CPT Jin S. Lee, A Co, 782d MI BN (CY)	15
Leading in Joint Cyber: Why Mutual Understanding Matters 1LT Prarabdha Yonzon, 782d MI BN (CY)	17
Integration in Action: Succeeding as an Army operating in a Joint Environment 2LT Mitchell Bardsley, B Co, 782d MI BN (CY)	19
Cyber Officer Leadership 1LT Joshua Williams, D Co, 782d MI BN (CY)	20
Marching Along As One: Strategies for Army Excellence in Joint Operations Major Ken M. Woods, Det. Texas, 782d MI BN (CY)	21
Training the Joint Force: How Army processes play an essential role in the Cyberspace Capability Developer (CCD) Work-Role CPT Mitchell Stiffler, D Co, OSE	23
AvengerCon IX returns to the Augusta Georgia Cyber Center 780 MI BDE (Cyber)	24

Attracting top talent and building relationships
780 MI BDE (Cyber)

Vanguard NCO Induction Ceremony
781st MI Battalion (Cyber)

Cyber Legion NCO Induction Ceremony
782d MI Battalion (Cyber)

Army Brigade Soldier Family Readiness Group
(SFRG) Assistant

HammerCon 2025, June 26
Military Cyber Professionals Association

Corkboard

In Memoriam: SSG Kurtis H. Beeson
781st MI Battalion (Cyber)

NEXT QUARTER'S BYTE recognizes our Army's 250th Birthday. For 250 years, Army Soldiers and civilians have supported our nation with their service. The central theme for the celebration is "This We'll Defend," which highlights the commitment of our Soldiers and civilians to defending our country, just as they always have. If you have an article to share, write a synopsis and send it to steven.p.stover.civ@army.mil NLT May 1, 2025. Final articles are due May 15, 2025.

27

29

31

33

34

36

43



The next issue of The BYTE, Volume 13, Issue 3, is a special edition, recognizing the Army's 250th Birthday, 1775 – 2025. The central theme for the celebration is "This We'll Defend," which highlights the commitment of our Soldiers and civilians to defending our country, just as they always have. Our campaign is focused on national public awareness and engagement effort to reach audiences at home and abroad, ensuring this is the largest and most inclusive commemoration in history.

Background: The Army's 250th birthday (2025) and America 250 (2026) provide the Army with several high-profile opportunities.

2025: The Army commemorates its 250th birthday throughout the year

2026: The nation commemorates its semi quin centennial with America250! celebrations

2025-2033: The U.S. Army Center of Military History commemorates the Revolutionary

Army Narratives:

Readiness. Our Army is lethal and comprised of cohesive teams that prioritize warfighting and delivering combat-ready formations. We rapidly project power to protect American and allied interests, ensuring our units are capable, equipped, and sustained. When the nation asks the Army to perform a mission, we have the speed and endurance to win.

Recruitment. The Army offers opportunities for present and future Soldiers and DA Civilians.

People. The human element is crucial for the Army's success. Approaching every interaction with compassion and a bias for action is fundamental.

Transformation. Our Army continuously transforms to outpace adversaries by leveraging the latest technologies for warfighting advantage through a framework of Continuous Transformation.

<https://www.americanrevolution.org/>

<https://www.army.mil/1775/>

<https://history.army.mil/Revwar250/>

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

v/r,

Steve Stover

Public Affairs Officer

780th MI Brigade (Cyber)

Editor, The BYTE





PRAETORIANS, As the global security environment becomes increasingly complex, the U.S. Army stands as a cornerstone of the Joint Force—working in seamless cooperation with the Air Force, Navy, Marine Corps, Coast Guard, and Space Force to ensure national security and global stability. This Byte issue explores the critical role the Army plays in a joint environment, highlighting how its success depends not only on its own readiness and capabilities but also on its ability to integrate effectively with the other services within the Joint Force.

Historically, the Army has operated primarily as a land-based power, with its own operational domains and mission sets. However, modern challenges, ranging from traditional combat to emerging threats in cyber and space, require the Army to collaborate across air, sea, and space domains. This cooperation allows the Joint Force to act with unmatched speed, precision, and adaptability.

In every domain, whether land, air, sea, or cyberspace, the Army's operational flexibility enhances the Joint Force's ability to execute complex operations at scale. This synergy is vital in achieving mission success, ensuring readiness, and maintaining strategic advantage. The Army's role goes beyond battlefield tactics—it includes leveraging cutting-edge technologies, enhancing interoperability, and fostering a culture of adaptability and mutual respect.

Through these pages, I invite you to explore the stories, insights, and strategies that define the Army's role within the Joint Force. These examples showcase the importance of collaboration, innovation, and unity, ensuring that the Army continues to evolve and succeed in an interconnected, dynamic world.

Very respectfully,
Candy Boparai
COL, CY
Commander, 780th MI BDE (Cyber)
"Everywhere and Always...In the Fight!" ■







11th Cyber Battalion “Leviathans” “Global Reach, Global Impact!”

By MAJ Vincent E. Michel, Information Advantage Cell Lead, 11th Cyber Battalion



THE ARMY’S PRIMARY PURPOSE is conducting land combat operations to defeat ground enemy forces and seize, defend, and occupy land areas, while also supporting four strategic roles for the joint force.¹ The four roles are preventing conflict, prevailing in large-scale ground combat, shaping the operational environments, and consolidating gains.² Additionally, the land domain is one of the most complex environments where nearly everything originates from the land, such as, capabilities, infrastructure, societies, to the opposing force, and operations in this domain require the ability to effectively operate across all domains.³ To successfully win in this complex environment it requires Soldiers, leaders, and units to have the requisite knowledge, skills, and attributes that can overcome ambiguity and chaos. Those skills and knowledge also ensure the forces provided to a combatant commander gives them multiple options to meet and overcome any challenges.⁴ The Soldiers and leaders within 11th Cyber Battalion have those unique skill sets and knowledge that contributes winning in a complex environment.

Since the activation of 11th Cyber Battalion in 2022, the Soldiers and leaders of the battalion have continued to hone their skills of conducting cyber and electromagnetic activities (CEMA) in support of land operations. This has taken the form of conducting rotations to combat training centers, where they have proven their ability to operate in the austere jungle environments of the Pacific, the swamps of Louisiana, and the Mojave Desert.⁵ During those rotations the Expeditionary CEMA Teams (ECT) showcased their technical and tactical knowledge by conducting radio frequency (RF) enabled offensive cyber operations (OCO) and electromagnetic reconnaissance (EMR),

while integrating with Army divisions and corps.⁶ By training and perfecting these tasks, the Soldiers of 11th Cyber Battalion have shown they can operate and win within the cyberspace and land domain, and provide a number of options to a commander that supports their scheme of maneuver. The cyber warriors of battalion have also shared their fundamental knowledge of CEMA operations with partner nations to build capacity, which highlights how one cannot forget a joint environment includes our partners and allies.⁷ These examples continue to emphasize that the battalion is a key organization that contributes to the Army’s ability to succeed in a joint environment. Furthermore, the battalion is the only expeditionary organization that can conduct both cyberspace and electromagnetic warfare, which “play an essential role in the Army’s conduct of unified land operations as part of the joint force.”⁸

Overall, cyberspace and the electromagnetic spectrum (EMS) are vital for success in today’s environment. The Soldiers of the battalion have proven that they can contest those spaces, while operating in austere environments. They have also shown that they can innovate at the tactical edge to overcome any challenges. They are using that innovative spirit back at home station to stand ready to win and are prepared to execute tactical actions that have operational impacts—which embodies the unit motto of “Global Reach, Global Impact.”

References:

- ¹Headquarters, Department of the Army (HQDA), Operations, Field Manual (FM) 3-0 (Fort Belvoir, VA: Army Publishing Directorate, 2022), 1-1, https://armypubs.army.mil/epubs/DR_pubs/DR_a/ARN36290-FM_3-0-000-WEB-2.pdf
- ²Headquarters, Department of the Army (HQDA), Unified Land Operations, Army Doctrine Publication (ADP) 3-0 (Fort Belvoir, VA: Army Publishing Directorate, 2019), 1-5, https://armypubs.army.mil/epubs/DR_pubs/DR_a/ARN18010-ADP_3-0-000-WEB-2.pdf
- ³Headquarters, Department of the Army (HQDA), The Army, Army Doctrine Publication (ADP) 1-0 (Fort Belvoir, VA: Army Publishing Directorate, 2019), 2-1, https://armypubs.army.mil/epubs/DR_pubs/DR_a/ARN18008-ADP_1-0-000-WEB-2.pdf
- ⁴HQDA, ADP 1-0, 2-1 to 2-4.
- ⁵Stover, Steven. 11th Cyber Battalion Support to JPMRC 25-01, <https://www.dvidshub.net/news/483426/11th-cyber-battalion-support-jpmrc-25-01>
- ⁶Stover, Steven. 11th Cyber Battalion supports U.S. Army Rotational Training Units at NTC 01. <https://www.dvidshub.net/video/951445/11th-cyber-battalion-supports-us-army-rotational-training-units-ntc-01>
- ⁷Grezzlik, Alisha. 11th Cyber Battalion Soldiers assist Moroccans with electronic warfare training at African Lion 2024. <https://www.dvidshub.net/news/471591/11th-cyber-battalion-Soldiers-assist-moroccans-with-electronic-warfare-training-african-lion-2024>
- ⁸Headquarters, Department of the Army (HQDA), Cyberspace Operations and Electromagnetic Warfare, Field Manual (FM) 3-12 (Fort Belvoir, VA: Army Publishing Directorate, 2021), 1-1, https://armypubs.army.mil/epubs/DR_pubs/DR_a/ARN33127-FM_3-12-000-WEB-1.pdf ■




11th Cyber Battalion supports U.S. Army Rotational Training Units at NTC



FORT IRWIN, Calif. — Bravo Company (Bandits), 11th Cyber Battalion, culminated months of home station training with participation in National Training Center Rotation 25-03, January 13 through February 7, 2025.

TRAIN HARD, FIGHT HARD, WIN EASY! GLOBAL REACH, GLOBAL IMPACT!

(U.S. Army photos by 1LT Angeline Tritschler).

#Army250 





FORT IRWIN, Calif. —Bravo Company (Bandits), 11th Cyber Battalion, culminated months of home station training with participation in National Training Center Rotation 25-03, January and February 2025.

Expeditionary CEMA (Cyber and Electromagnetic Activities) Team 05 and ECT 06, B Co., 11CB, executed shaping operations during the rotation that set conditions for 1st Infantry Division and 3rd Special Forces Group (AIRBORNE) offensive and defensive operations.

“Leviathan CEMA Warriors led the way in demonstrating how to leverage Cyber and Electronic Warfare capabilities to deliver effects that enable the lethality of ground maneuver forces on the battlefield,” said Lt. Col. Louis Etienne, commander, 11th Cyber Battalion.



FORT IRWIN, Calif. – Distinguished visitors view static displays featuring various equipment used by Soldiers in 11th Cyber Battalion, January 25.

"I want to express my gratitude for all the CEMA Leaders and Stakeholders who either came to observe 11th Cyber Battalion's training during National Training Center rotation 25-03 or participated in our Distinguished Visitors Day.



CEMA Leaders from across the Army got to see firsthand why 11th Cyber Battalion is such an effective fighting force...the amazing Soldiers who get after it every day!" LTC Louis Etienne, commander, 11th Cyber Battalion.
TRAIN HARD, FIGHT HARD, WIN EASY! GLOBAL REACH, GLOBAL IMPACT!
(U.S. Army photos by 1LT Angeline Tritschler).
#Army250 #ArmyCyber ■

Army Leadership in a Joint Environment

By LTC Thomas Schindler, 781st MI Battalion (Cyber)



The joint service color guard displays the American and service flags during the 2015 USO Gala in Washington, D.C., Oct. 20, 2015. U.S. Marine Corps photo by Sgt. Gabriela Garcia

JOINT PUBLICATION 3.0 DEFINES JOINT OPERATIONS as the primary way the Department of Defense employs two or more Services in a single operation. According to doctrine, the Army is the dominant U.S. fighting force in the land domain. Army forces both depend upon and enable the joint force across multiple domains, including air, land, maritime, space, and cyberspace. Members of the 780th MI Brigade frequently must engage, work with, and leverage members of other Services to ensure the mission and objectives of the operation are achieved.

Working in a joint environment presents different challenges and conflicting requirements. Each Service has their own requirements (yearly training, weapons qualification, professionally military education, etc.) that their members must go through. These conflicting requirements are generally the biggest challenge. Soldiers and Civilians are expected to meet the operational requirements from the Joint

Force Commander, while balancing the administrative requirements of their services. In a typical Joint unit, most billets are managed by a Joint manning document. The Cyber National Mission Force (CNMF) however, is not fully manned by Joint billets and instead, most of the combat power is "borrowed" from the Army, Air Force, Navy, Marines, and the Coast Guard. This creates an ADCON vs OPCON disconnect that makes it difficult to balance the conflicting requirements of the services, and of the CNMF. The ones who are affected the most by this are the junior personnel who are stretched thin by operational demands and ADCON responsibilities.

Navigating a dual-hatted environment with two separate chains of command presents a unique set of challenges. Reporting to two distinct organizations with "joint" responsibilities, yet different administrative controls, creates confusion regarding communication and guidance. Discrepancies in work schedules, physical training expectations, and task prioritization

can lead to uncertainty. This ambiguity is further complicated by differing service event calendars, ensuring work center coverage, and separate rating systems that make performance evaluations difficult and potentially inconsistent. Ultimately, the lack of a unified approach to corrective actions allows for accountability gaps.

Differing Service cultures contribute to friction within joint environments. Each Service operates with its own distinct communication style, organizational structure, and operational tempo, often leading to a steep learning curve for personnel new to inter-service collaboration. While not insurmountable, these cultural nuances can create misunderstandings. For instance, the Navy's classification of O4s as "junior officers" contrasts sharply with the Army and Air Force's view of them as seasoned leaders. Similarly, the gravity assigned to written counseling varies significantly; a mere formality in the Army and Air Force, while carrying significant weight within the Navy's disciplinary system. These subtle



yet impactful differences underscore the importance of cultural sensitivity and open communication to bridge the gap between service cultures and foster a cohesive joint environment.

Further complicating the joint environment are inconsistencies in training and expertise levels across services. While all branches strive for excellence, variations in professional development opportunities and operational priorities inevitably result in a diverse range of skill sets within a joint team. For example, the Army's tendency to empower NCOs at lower ranks often translates to a higher level of practical experience compared to their Navy and Air Force counterparts of the same grade. This disparity can lead to awkward situations where junior personnel are tasked with leading or mentoring more senior members from other branches. Different services also train differently than each other, leading to a wide range of technical talent on the teams. Budgetary constraints further exacerbate these issues by limiting access to specialized training and professional development opportunities, ultimately hindering the development of a cohesive and highly skilled joint force.

The United States Army was established in 1775, and since then has developed a unique identity that encourages character,

integrity, and selfless service. When working in a Joint environment, Soldiers and their families are introduced to a new set of strong traditions and values from other services and while this is one of the best aspects of a Joint environment, it's important to maintain our Army Identity. This can be difficult due to ADCON vs OPCON dilemma discussed earlier, but the 781st MI BN has made great strides reducing the gap between the Battalion and CNMF while maintaining its identity. Part of this success can be attributed to concerted effort by the Battalion to host regular townhalls and morale days along with traditional Army ceremonies like an NCO induction ceremony. These events while they may seem small, bring our Soldiers together to celebrate our comradeship that is unique to the Army. It is vital that Army leaders promote and encourage the unique aspects of our service that make our Soldiers the cyber professionals they are.

Joint environments, while designed to leverage the strengths of each military branch, present significant challenges due to inherent inconsistencies. Different chain of commands, cultural norms, leadership expectations, and approaches to discipline create confusion, complicate communication, and hinder accountability. Additionally, inconsistent training and professional development opportunities

across services, often limited by budget constraints, result in a mismatch of expertise levels within joint teams. These disparities underscore the need for standardized procedures, cultural sensitivity awareness, and equitable access to training to foster a cohesive and effective joint force. Despite the challenges, the Joint environment creates opportunities for success that leverage the unique experiences, culture, and skills each service brings to the table. Finally, maintaining individual service identities within a joint environment is crucial, with efforts like those of the 781st MI BN demonstrating how to bridge inter-service gaps while preserving unique traditions and values. ■

Bridging the Divide; Cultivating Success in Joint Military Operations

By 1LT(P) Stephen Romer, 781st MI Battalion (Cyber)

WE ARE ALL acquainted with the ever-familiar Joint Publication 3-0. I've had to read it, and you the reader have, most likely once had to skim its pages (or for the more intrepid reader- read it cover to cover). JP 3-0 defines joint operations as "Military actions conducted by joint forces and those Service forces employed in specified command relationships with each other, which, of themselves, do not establish joint forces." Pretty simple, straight forward definition one would say. If we, however, interpret this from the standpoint of a Junior Army leader, one could argue it fundamentally says "You, as an Army leader, will at one point suddenly find yourself working hand-in-hand with Marines, Sailors, Airmen, Guardians and/ or Coast Guardsmen to accomplish a collective mission. By the way, Sergeant/ Chief/Sir/Ma'am, good luck".



Figure 1: DoD Armed Service Logos. (DoD)

In this article I will argue that good joint operational leadership is more than what is written down in doctrine—it is the ability to synthesize mission success while also tackling the balance and mitigation of adjacent service component paradigms and all that comes with it.

"Creative solutions to hard problems" are what joint operations hope to achieve, and to become more effective at our job as a leader of in the joint service, we need to

understand the joint environment in which joint service lives and breathes. In this space, the mixture and sometimes clashing of service component paradigms can become apparent relatively quickly. Clashing of ideas, procedures and expectations are all things that feed innovation, helping with creative solutions, but being set in the rigidity of comfortable norms, can stifle it—and that itself is a "hard problem" for joint service. This "hard problem" can all be traced to the paradigms or *modus operandi* in which these service components practice. Paradigms are fed by the culture, norms and collectively understood interservice standards in each branch. Whether we admit it or not (or if you have served in more than one branch for a significant amount of time), we all fall into this trap-- The Army does things the Army way; the Marines, The Corp way, etc., and if you ask each of them separately who does things the right way, I would bet they all would say "We do!". If we recognize this bias, we as Army leaders will arguably become more comfortable being uncomfortable and therefore lethal while engulfed in the entropy of joint service. Becoming the standard bearers for what it means to lead in a joint operational environment is what we should all strive for as Army leaders.

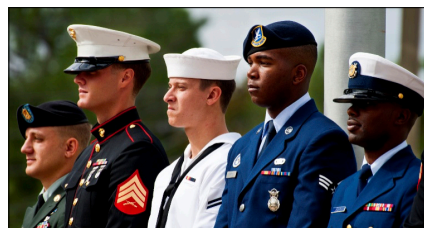


Figure 2: Joint-service honor guard members representing all five military services stand in front of the audience before the outdoor portion of the POW/ MIA ceremony Sept. 16 at the Air Force Armament Museum (U.S. Air Force photo/Samuel King Jr.)

"Bridging the Gap" is the title that was chosen for this article, and like most things, I think the main answer to cultivating cohesion between service components (i.e. bridging the gap) and mitigating any rifts that come with joint service, is done first and foremost taking care of the people. The following points are some tips that have been passed down to me by multitudes of Officer, Warrant and Enlisted leaders:

- **KNOW** their eval process: (Ex: FITREPs v NCOERs v. OERs v. Performance Briefs) Knowing how each of the service members (SM) are rated in the branches is an invaluable skill you will need sooner or later. Finding yourself having to provide bullets for a Junior Sailors/Marine's FITREP and not knowing the writing style or system of record, or that you would even be in their rating chain could unfairly stifle the development of that SM. Just like we have rating chains written down in the Army, take the time on the side to develop a plan and visualize the timelines of your SMs. Having to scramble at the last minute to ultimately come up with a half-baked eval, puts unnecessary burden and stress on all those involved and does a disservice to the force.
- Get to know their culture and lingo: (Ex: Hoorah vs. Oorah vs. Hooah vs. Hooyah; Battle Buddy v. Shipmates) (Ex: Promotion ceremonies vs wetting downs; pinning vs. making rate)

Culture and traditions are important. By showing interest in adjacent service components culture through their lingo, ceremonial procedures and the like, you will build morale and just show that you plain care. All services have their own lingo-- it's a huge part of all military



culture and the vocal representations of who we are and why we do things the way we do.

Know their ranks and how to identify uniforms: (Ex: Master Chief vs. Senior Chief vs. Airforce Chief vs. Army Chief Warrant) (Ex: Navy admirals and other senior officers by their stripes/collars.)

There are few things more embarrassing to experience than seeing a Senior Naval Officer in their dress uniform walking towards you and slowly realizing, as they get closer, that you have absolutely no idea how to gauge what their rank is. Most in this situation (though they won't admit it) ultimately opt to pick a rank (probably Admiral) that they think is right, salute/mumble a greeting of the day, and pray they are far too busy to give it any mind. Avoid this; take the time and look at the guides online for each components rank structure and presentation on uniforms

(dress or otherwise). You'd be surprised by how much favor you can garner with services by confidently addressing them by their proper terms.

- Ask questions to your joint service peers.

Not being afraid to ask questions to your fellow joint-service members is consistent guidance that will get you more clarity and help stave off the firehose you will be drinking from. In the Army we live and breathe acronyms, and this is ramped up to an "11" in the joint environment. If you do not know what something means or stands for, ask the question! Conversely, once you know what a term means, or acronym stands for, help give back to the service by passing your findings to your fellow Army Soldiers and Officers. Continuing the cross pollination of knowledge to those coming up after you will ensure less knowledge gaps and

expedite the "flash-to-bang" of effective planning and communication, ensuring better odds at mission success

In conclusion, joint operational service is tough and can at sometimes might feel like you are learning to be in the military all over again. It however is a challenge that we as Army leaders can not only rise to meet but push the boundary of excellence and set a new standard for others to follow. We consistently preach "One team, one fight" and while we do it well, it's time for us to ascend to the next plateau. ■



Figure 3: Joint service personnel and Djibouti port authority take part in first ever Djibouti port exercise. (AFRICOM)

Giving Due Credit in a Joint Environment

By 1LT Matthew Holcomb, Operations Officer, 781st MI Battalion (Cyber)

THERE IS VITAL importance in recognizing the exemplary work of our servicemembers. As leaders, we are called to use awards to “foster mission accomplishment by recognizing... and motivating [servicemembers and civilians] to high levels of performance and service” (Army Regulation 600-8-22, Military Awards). Recommending and granting awards are tools afforded us to award dutiful service, improve job satisfaction, and point to what right looks like. But, in joint environments, too often these same marks of pride can create unrest instead. Leaders in these circumstances must take additional steps to ensure their inter-branch subordinates are offered the same opportunities for recognition as their inter-branch peers.

Last year, I recommended an operations team consisting of Soldiers, Sailors, and Airmen for achievement medals. After months of dedicated preparation, their flawless execution supported a critical objective, and I was confident that their efforts had earned them a recommendation. I consulted each branch’s doctrine governing military awards, submitted, and waited. Army leadership decided that this accomplishment deserved an elevated award and presented the Soldiers with Army Commendation Medals. Air Force leadership agreed with the recommendation and awarded an Air Force Achievement Medal. Navy leadership disagreed with the recommendation, reducing the award to a Certificate of Appreciation. Why would the same achievement elicit such different results? After the results of my awards came back, I petitioned the Navy commander once more, citing the parallel accomplishments of the Sailor and their peers. Finally, I pivoted to get the Sailor recognition through other means, eventually earning him an award through their joint leadership.

Each branch’s doctrine agrees, it is the commander’s discretion to grant awards. Every commander develops their own

command philosophy, assigning criteria for what does and does not qualify for decorations. Junior leaders therefore must quickly learn to discern what accomplishments apply to those criteria and make award recommendations accordingly. Navigating the differing instructions of service regulations, commanders’ guidance, and precedents will remain a complicating factor for leaders in a joint environment. Faced with these unique challenges, leaders in a joint environment are called to identify creative solutions for giving deserved recognition. For instance, servicemembers permanently assigned to a unit or organization of another military department could qualify for the awards in the assigned unit’s branch rather than their own. Servicemembers occupying joint billets could qualify for Joint Service Achievement and Joint Service Commendation Medals regardless of their branch of service. Foregoing decorations, coins, plaques, or public displays of recognition are also consistently effective means of appreciation for high achievers.

What is important is that no servicemember works hard, distinguishes themselves, but receives no indication that they are appreciated. Even though getting awards for servicemembers in other services demands added effort, doing so is necessary to build motivated teams from a breadth of backgrounds. Leaders should therefore stay engaged with the services’ doctrines and command cultures to get their people recognized for meritorious service.

References:

DoD Manual 1348.33 Manual of Military Decorations and Awards: DoD Joint Decorations and Awards
SECNAVINST 1650.1 Navy and Marine Corps Awards Manual
DAFMAN 36-2806 Military Awards: Criteria and Procedures
Army Regulation 600822 Military Award ■





Vanguard Battalion Relinquishment of Responsibility – Farewell to a Beloved Leader

FORT GEORGE G. MEADE, Md. – The Soldiers and Civilians of the 781st Military Intelligence Battalion (Cyber), Vanguard, and 780th Military Intelligence Brigade (Cyber), Praetorians, bid a bittersweet farewell to Command Sergeant Major Jermaine Ocean, who relinquished his responsibility as the battalion's senior enlisted leader and "keeper of the colors", and this ceremony also served as his retirement ceremony after 25 years of faithful and dedicated service to our Nation.

The ceremony also recognized Command Sgt. Maj. Ocean's Family, as they too have sacrificed and served our Country in their own special way.

Vanguard... When Others Cannot

The relinquishment of responsibility is a simple, yet traditional event that is rich with symbolism and heritage. The key to the ceremony is the passing of the colors. The very soul of a military unit is symbolized in the colors under which it fights for they represent not only the lineage and honors of the unit, but also the loyalty and unity of its Soldiers. The custodian of the colors is the Command Sergeant Major, who is the senior enlisted Soldier in the unit and principal advisor to the commander.

"I'm not going to go through the details of his long and storied career from whether it was standing up the Cyber National Mission Force, Cyber Branch, creating 23 National Mission Team, being a command sergeant major of this battalion," said Lieutenant Colonel Scott Beal, commander of the 781st MI Battalion. "What I am going to explain to you is what my friend and brother Jermaine has meant to me, and I will attempt to articulate how every one of you feel about him.

"There's not a day that goes by that Jermaine spends more than five, maybe ten minutes in his office at any given time," added Beal. "He's the type of command sergeant major who is where the Soldiers

are, where the Civilians are, where the contractors are; he's a Soldier's Soldier. He wants to be where you work. He wants to talk to you, he wants to see you, he wants to hear you, and he wants to solve your challenges and celebrate your victories and help you overcome whatever struggles you might be going through in your life."

Command Sgt. Maj. Ocean dedicated a quarter of a century to distinguished service in the United States Army. His career, beginning in 1999 spanned a remarkable journey across various leadership roles and duty stations around the globe. He continually sought professional development, amassing an impressive range of military education and certifications, for his exemplary service and unwavering commitment he was recognized with numerous awards and decorations.

"For those of you who don't know, back then in 2013, we were just building the teams, and Sergeant Major Ocean, his fingerprints are all over the build of all of the teams," said Colonel Candy Boparai, commander of the 780th MI Brigade. "That is the legacy he leaves behind... That is something all of us in the Cyber Force will know."

Col. Boparai presented Command Sgt. Maj. Ocean with the Legion of Merit, his retirement pin, Certificate of Retirement; and following the ceremony, he was presented his U.S. flag, commemorating his retirement, from the interim battalion senior enlisted leader, First Sergeant Daniel Ingle.

"The position I'm in... I look at everybody in this organization, whether you're in uniform, contractor, Civilian, whatever the case may be, I look at you as my child and it's my responsibility to make sure you have everything you need to succeed," said Ocean. "I can't say thank you enough to the Soldiers, Civilians, contractors of the 781st. My intent every day was just to come to work every day and give it everything I could possibly

give."

Command Sgt. Maj. Ocean reminisced about, when he a kid, his mom told him when you go to sleepovers, you always leave a place better than you found it.

"When you're in certain positions, in this position particularly, I think about stuff like that, and my thought process from the time I took this seat to the time to now, was to always leave the place better than where I found it... and I hope I did that."

Towards the end of his poignant remarks, Ocean said, "I care about the people ten times more than I care about the mission, and I probably shouldn't say that, but it is what it is. The mission's going to get done one way or another. The people are the important part."

"With that, my final transmission, Vanguard 7, signing off."

#Army250 #ArmyPossibilities ■





How Combatant Command Cyber Protection Team (C-CPT), 503 CPT, Task Organized to Support Joint DCO

By CPT Jin S. Lee, A Company, 782d MI Battalion (Cyber)



Executive Summary

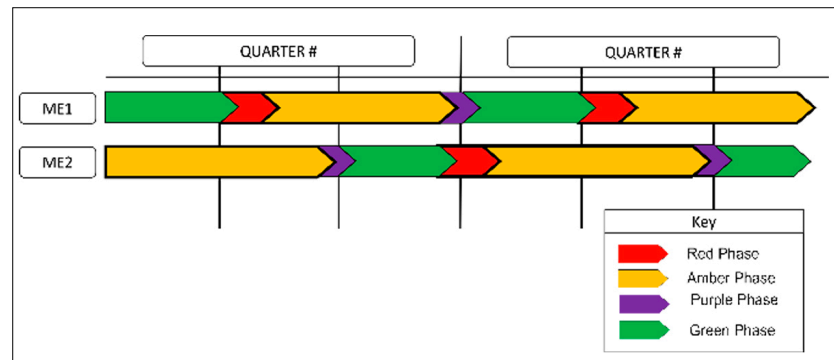
503 Cyber Protection Team (CPT) is one of the four (4) combatant command teams (C-CPT) within the 1st Cyber Battalion (1CYBN). 503 CPT is tactical control (TACON) to Joint Task Force Cyber (JTF-C), operational control (OPCON) to Joint Force Headquarters Cyber (JFHQ-C) Navy, and administrative control (ADCON) to 1CYBN. This paper provides information on how 503 CPT utilizes the CWP 3-33.4 three (3) mission elements (ME) and support elements (SE) model to task organize its forces to maximize the flexibility between OPCON and ADCON task and mission requirements.

Introduction

By design, the structure of CPT allows interoperability to train and deploy MEs on any mission. 503 CPT employs their ME using the sustainable readiness model (SRM) to set mission readiness, battlefield preparation, and training guidelines to enable ME's mission deployment. In addition, the SE provides the necessary analytical, technical, and training support to assist ME mission success. This paper will further discuss the essential tasks the ME and SE are responsible for to meet all operational and administrative requirements.

Operational Cycle

503 CPT utilizes the SRM to maintain a continuous battlefield preparation while on the OPTEMPO mission schedule. Compared to 2CYBN, the 1CYBN grants CPT Team Leads (TL) the controls to determine the length of each phase for the mission element. OPCON requirement shapes the structure of the 503 CPT's SRM.



The diagram shows the timeframe of each phase of the SRM for both MEs. The 503 CPT's SRM consists of red (mission recovery), amber (mission preparation), purple (mission staging), and green (mission) phases. The SRM is structured to balance the OPCON and ADCON duties between two MEs. First, the ME supplies the team with ADCON tasking support during the amber phase. Then, the ME prioritizes the OPCON requirements during the green, pre-mission, and post-mission phases. Throughout the cycle, the SE oversees both MEs and supports training and mission success. In addition, the SE handles all communication between the mission owners, OPCON, and ADCON commands for the MEs.

Red Phase

The goal of the phase is to provide the ME with 14 days to tackle administrative, personal responsibilities, and post-mission recovery. Concurrently, The CPT leadership and SE begin the mission analysis for the next mission. The TL issues a warning order (WARNO) to the ME to start their Troop Leading Procedures (TLP). The WARNO provides the understanding of the operation and coordinating instruction for the ME and SE. With the set guideline established, The ME and SE conduct training sync meetings to develop

a mission readiness plan to close any operational gaps. The SE provides the ME with the mission's intelligence, including any Advanced Persistent Threats (APT), basic network description, and a battlefield analysis. The CPT leadership, including the ME lead, identifies the timeframe of the operation, necessary equipment, and personnel needed for the mission.

Amber Phase

The amber phase occurs for 30 days after the red phase. The ME provides ADCON tasking support while conducting mission readiness training in preparation for the upcoming mission. The phase began with SE providing the ME lead with a mission-essential checklist. The list provides all the administrative and logical requirements for the operation. Concurrently, the mission owner and CPT leadership start a mission workgroup to discuss and refine the mission. Next, SE provides the team lead with an Intelligence Preparation of the Battlefield (IPB) briefing to provide a strategical and tactical battlefield overview. The driving focus of the workgroup is to establish communication with the mission owner and submit a request for information to characterize the physical and logical area of the battlefield. The exchange of mission ownership from the SE to the ME occurs after publishing the team's Operation

Order (OPORD) and an initial draft of the analytic scheme of maneuver (ASOM). The ME, with the support from SE, refines the kill chain and the mission ASOM. In conjunction with the SE effort of work, the ME utilizes the team's master gunner (MG) and technical advisor to provide ME-level training using the Persistent Cyber Training Environment (PCTE), CMU Cyber force, and internal lab environments. The phase ends when all the mission essential tasks are met and verified by the CPT leadership for ME deployment.

Purple Phase

Before the green phase, the ME has 14 days of pre-mission staging in preparation for the mission. All ADCON requirements are removed during the purple phase to focus on OPCODE requirements and ensure mission success. The phase ends when the ME is staged and ready for mission deployment.

Green Phase

In the green phase, the priority is mission and mission support and battle tracking for the SE. Usually, 503 CPT forward deploys a ME for 30 days or less, depending on the mission scope or OPCODE's requirements. Any mission that requires more than 30 days will be subject to review by the OPCODE and the CPT leadership to extend the mission timeframe. In case of extension of the mission, the CPT TL has the authorization to exchange mission ownership between two MEs. As a result, the incoming ME will be given adequate time to assume mission command.

Conclusion

The functionality of the SRM provides the flexibility for the TL to train and deploy ME to support OPCODE and ADCON taskings. Utilizing the model offers great control for the ME to have plenty of time to prepare, refine, prep, conduct a mission, and recover. Foremost, phasing out the cycle allows the CPT leadership to plan Soldier readiness and organize the priority of work to enable mission success..

References:

1. Joint Publication 3-12 Cyberspace Operations
2. Cyber Warfare Publication (CWP) 3-33.4 -Cyber Protection Team (CPT) organization, function, and employment

Contributors – Thanks to the following individuals for contributing their time and expertise to this paper. Their input was invaluable.

- LTC Major, Keith
- CW2 Parson, Joshua
- MAJ Godwin, Michael
- CPT Abeledo, Roberto

Their input was considered, but this paper is not necessarily an accurate reflection of their opinions.

About the author – CPT Lee was born in Incheon, South Korea, and grew up in Burke, VA. He commissioned at Virginia Military Institute (VMI) through its Reserve Officer Training Corps (ROTC) program in August of 2018 and completed Cyber Basic Officer leaders Course (BOLC) at Fort Eisenhower. He has held numerous leadership and development positions to include Headquarters, Department of the Army (HQDA) G1 IPPS-A Sr. Developer, HQDA G1 IPPS-A Data Officer, 503 Cyber Protection Team (CPT) Analytic Support Officer (ASO), 150 CPT Mission Element (ME) Lead, 15th Signal Brigade S3 Assistance Task Officer. CPT Lee's military school include CYCCC, CYBOLC, Army Space Cadre I and II courses, and How the Army Run Course (HARC). His awards include Meritorious Service Medal (MSM), Army Commendation Medal (ACM), Army Achievement Medal (AAM), National Defense Service Medal, Global War on Terrorism Service Medal, Army Staff Identification Badge. ■



Leading in Joint Cyber: Why Mutual Understanding Matters

By 1LT Prarabdha Yonzon, 782d MI Battalion (Cyber)

THE MODERN battlespace is seldom fought in isolation. Instead, it demands coordination not only across multiple domains but also across joint forces and branches. In this environment, achieving success relies on understanding and harmonizing unique cultures. This is clearly evident in combat arms roles. In distinct platforms such as fixed-wing close air support and Army infantry operations, leaders must build trust to harvest the true capability of multi-domain operations. However, in cyber—where operations look similar across military branches—cohesiveness becomes misleading. In an environment where integration is seamless, seeking to understand another's unique culture can seem negligible. In reality, overlooking subtle differences impedes the ability to use the full potential of joint cyber collaboration. Thus, it is vital that in a joint-effort cyber environment, leaders must understand the demands, strengths, and differences which exist in each branch, building trust that allows them to effectively anticipate and face the operational challenges ahead.

In traditional combat roles, differences between the military branches become clear, as seen with coordination between Air Force close air support and Army infantry operations. Though the Army has organic aviation assets, the use of close air support is outsourced from other branches, such as the Air Force. In “Multi Domain Operations and Close Air Support,” Lt. Col. Clay Bartley, Maj. Time Tormey, and Dr. Jon Hendrickson explain that platforms such as the F-35 and A-10 play a pivotal role in multi-domain operations. Specifically, they state that an effective multi-domain approach is rooted in mutual understanding and trust, stating, “the first step toward achieving increased trust is a common understanding of multi-domain operations.” Without

understanding the importance and use of each crucial component in war—such as close air support and infantry operations—multi-domain operations risk failure. In this example, the Army is not equipped to provide the level of close air support necessary to enable many operations, while the Air Force is. Thus, careful understanding and coordination between branches becomes necessary. While these stark differences between branches highlight the importance of mutual understanding, cyber operations pose a different challenge. The presence of well-defined branch-agnostic cyber roles simplifies integration but also creates a dangerous facade that trust and coordination are already established.

Cyber synchronization between branches exists organically. In offensive cyber operations, cyber roles and standards are shared among branches. In the Army Basic Officer Leadership Course (BOLC)—the first cyber primary education required by Army cyber officers—doctrine from joint publications is taught. Through the foundation of instruction, joint integration is embedded in Army cyber. Furthermore, Bartley, Tormey, and Hendrickson further emphasize this point, arguing “the [individual] component lens is not sufficient in [multi-domain operations] because operations are too complex.” Cyber efforts do not fit neatly into traditional joint efforts such as Army infantry operations and close air support. It is important to note, however, that there are clear differences between Joint Force Headquarters and priorities amongst branches. That said, the foundational concept between headquarters remains the same: cyber efforts are led by joint forces in mainly branch-agnostic cyber roles. As a leader coming into this environment, integration seems at times flawless. An Army exploitation analyst could work in tandem with a Navy operator with no

need to bridge a gap in branch-specific knowledge. Instead, they operate by understanding the project, their role, and the requirements for success. In this environment, leaders may be led to believe that there is no need to invest time to understand the nuances between branches, even at the tactical level.

This seamless integration can cause leaders to overlook branch-specific nuances, creating operational blind spots. Although cyber roles are rarely branch-specific, each service component inherently interprets mission requirements with unique schemas. For example, in the Army, leadership training, regardless of branch, revolves around ground combat operations, reinforcing a perspective centered on land warfare. In contrast, the Air Force, whose core mission is built around aviation platforms, has a different frame of reference when teaching leadership. Though effective leadership qualities amongst any frame of reference share similarities, these nuances generate different perspectives. For example, risk management decisions made by an Army exploitation analyst may differ from a Navy counterpart. Even though they share the same job qualifications, their frame of reference is inherently different. Additionally, each branch promotes different expectations for its personnel. In the army, commissioned officers can take on technical roles such as operator, but they are still required to fulfil traditional leadership obligations, highlighted during key development (KD) positions. While this balance is understood in the Army, these competing demands may not be as clear to an Air Force task force commander overseeing Army personnel. Similarly, each branch has unique requirements which shape how service members may operate within the joint environment.

It is vital to understand these nuances as an Army, for we will continue to work in

tandem with other branches in joint cyber missions. By understanding requirements and demands across the board, we can make more informed decisions, foster collaboration, and, most importantly, build mutual understanding and trust—strengthening cyber integration across the joint force.

References:

¹⁴Bartels et al., *Multidomain Operations and Close Air Support: A Fresh Perspective* 2017.

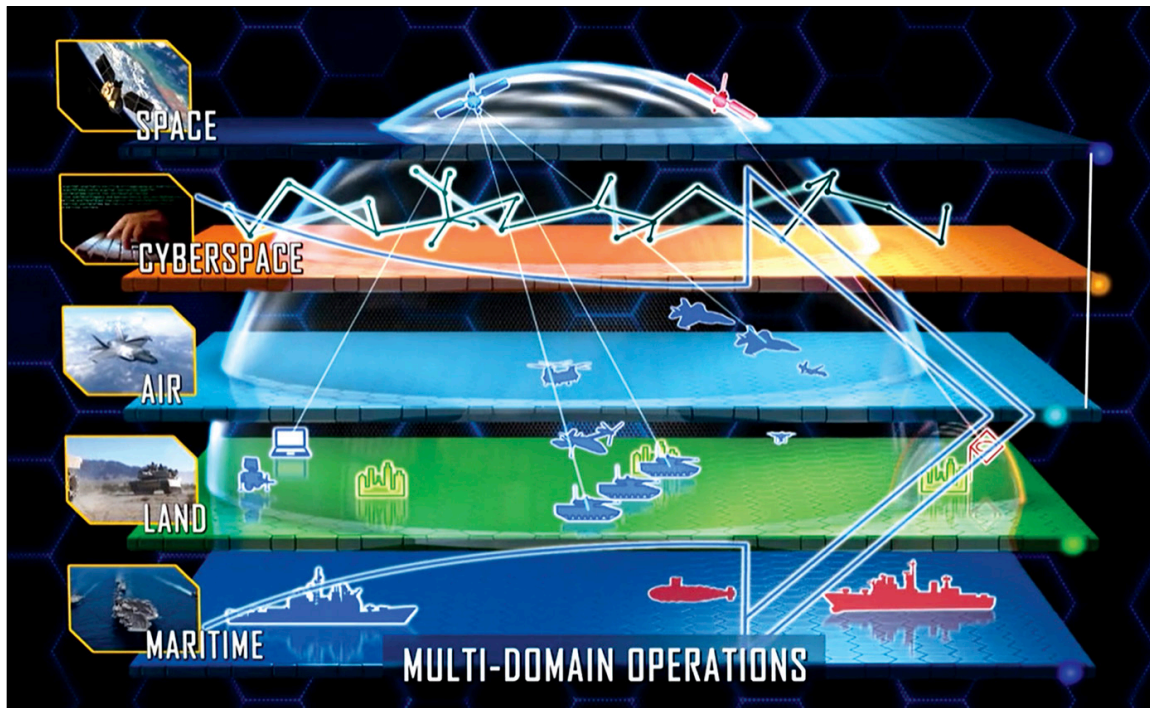
¹⁵Bartels et al., *Multidomain Operations and Close Air Support: A Fresh Perspective* 2017

Bartels, C., Tormey, T., & Hendrickson, J. (2017, March). *Multidomain Operations and Close Air Support: A Fresh Perspective*. Army University Press. <https://www.armyupress.army.mil/Journals/Military-Review/English-Edition-Archives/March-April-2017/ART-011/> ■



Integration in Action: Succeeding as an Army operating in a Joint Environment

By 2LT Mitchell Bardsley, B Company, 782d MI Battalion (Cyber)



OPERATION OVERLORD marked a pivotal moment for the world, when the United States, United Kingdom, Canada, and the Allied nations unified under one command structure and conducted the largest amphibious assault in history, combining infantry troops on the beaches, airborne troops capturing strategic objectives behind enemy lines, naval transportation and fire support, and extensive air support and bombing runs by the U.S. Army Air Forces and Royal Air Forces. This elaborate-yet-synchronous operation was underpinned by the Allied War and Defense Departments, providing consequential intelligence along with conducting deception and sabotage missions. These supporting elements proved decisive to heavily securing the preparation and execution of D-Day.

Today, the joint environment is expansive, and the information domain is never-ending, by comparison. A plethora

of sensors, open-source information, and decentralized and near-peer threats require detailed, robust, accurate, and integrated intelligence. Simultaneously, information warfare could not be waged without a powerful and effective cyber force to maintain the U.S. multi-domain advantage and inform critical decisions in the uniformed services, as well as in the Intelligence Community and between our allied nations. An incomparable cohesion in developing a shared understanding and projecting power as one effort will guarantee success in delivering the National Defense Strategy through competitive and complex modern warfare.

The U.S. Army achieves mission success by synergizing the employment of multi-domain capabilities, particularly in cyber domain dominance, executing robust joint training exercises focused on Large Scale Combat Operations (LSCO), and endorsing innovative leadership at all echelons. The Army's ability to collaborate,

communicate, plan, and successfully deliver effects in joint environments stems from blending traditional combat power and maneuver tactics with state-of-the-art cyber strategies and capabilities. The coordinated planning and use of joint and interagency information resources, capabilities, and activities strengthens a "one team, one fight" approach, delivering defensive, offensive, and exploitative effects. This enables operational and strategic success within the incredibly contested modern information environment.

References:

Image Source: <https://www.armyupress.army.mil/Journals/Military-Review/English-Edition-Archives/November-December-2021/Ryder-Domain-Awareness/> ■

Cyber Officer Leadership

By 1LT Joshua Williams, D Company, 782d MI Battalion (Cyber)

THE U.S. ARMY cyber branch is distinctive in that it offers a wide variety of assignments for Junior Officers in accordance with DA Pam 600-3. This contrasts with other basic branches, which often have a clearer career trajectory. With these assignments existing on a spectrum that has leadership on one end and technical capabilities on the other, it can be difficult for Junior Officers to fully understand their *raison d'être*. While Army Cyber Officers must develop a solid technical acumen, balancing this with a strong focus on leadership development is imperative to achieve success in a joint environment.

The Cyber Branch is particularly alluring to many cadets and officer candidates because it aligns their professional desire to serve as Army Officers with their personal and academic interests in the cyber domain. My initial attraction to the Cyber Branch stemmed from my experience as a Systems Engineering major at West Point, where I took multiple intellectually stimulating classes as part of a Cyber Security Systems elective track. Therefore, when going through the talent-based branching process during my senior year, I pursued an Army career where I could leverage my academic background. To earn a spot within the branch, I had to complete two interviews that assessed my leadership capabilities and personal attributes, as well as my technical background. Upon learning months later that I would become an Army Cyber Officer, I felt excited to continue developing the competencies necessary for success. My experience reflects a broader trend among many prospective Officers, whose strong interest in what the Cyber Branch offers encourages them to pursue a somewhat nontraditional career path.

Although the Cyber Branch understandably emphasizes technical capabilities during the branching process, future lieutenants may develop inaccurate expectations of their role within the

branch. The Cyber Basic Officer Leader Course (CyBOLC) has various technical modules that are fast-paced, and having a cyber-related background anecdotally makes it substantially easier to learn new concepts. Furthermore, Junior Officers in the Cyber Branch must understand the work of the Soldiers they lead. Therefore, it is reasonable for the branch to select cadets and officer candidates who have, or at least have the propensity to develop, a solid technical foundation that leads to career success. All Officers have their own individual goals, but it is imperative for those who want to make a career out of the Army to avoid the trap of desiring purely technical roles, as this can lead to disappointment in the long run.

The reality is that most Junior Officers are not “on-keyboard.” In fact, many serve in more traditional assignments that are ostensibly not operationally related to cyber at all, such as Advanced Individual Training (AIT) Platoon Leader, Battalion Staff, or Company Commander. Even Junior Officers who do serve on Cyber Mission Force (CMF) teams, such as myself, often assume assignments where we lead Soldiers in highly technical work roles. Furthermore, despite there being lieutenants and captains who serve in technical assignments, this becomes very uncommon as one progresses in their career. Although all career Cyber Officers ultimately will take on assignments that do not fully leverage their technical background, I believe it is important that we understand our role in the broader context of our mission.

While Cyber Officers are undoubtedly technical professionals, we are first and foremost leaders responsible for enabling cyberspace operations. Our leadership is essential to enable effects within a dynamic joint environment. Enlisted Soldiers, Warrant Officers, and DA Civilians in the CMF are highly technical and proficient in executing these effects, but Officers play a critical role in successfully integrating

them into an operational environment that requires coordination between different units, branches, and organizations. This often involves communicating with joint force headquarters or mission partners who might not fully understand the organizational context of the Army. Regardless of their assignment, Officers have a unique opportunity to develop the analytical and problem-solving skills necessary to ensure this symbiotic relationship between our teams and external organizations. Even Officers who are Exploitation Analysts or Interactive On-net Operators contribute to this relationship by utilizing their technical expertise to further decrease ambiguity within an often-convoluted organizational network. Overall, Cyber Officers facilitate success in a joint environment by employing our soft and hard skills to navigate the complexities inherent to joint military operations.

Ultimately, while the Cyber Branch provides Officers with the ability to map out an exciting career path, it is imperative to realize that technical proficiency is just one aspect of this ever-changing field. As a Lieutenant who is relatively new to the branch, I am eager to continue exploring the balance between honing technical skills with leading in a joint environment. ■



Marching Along As One: Strategies for Army Excellence in Joint Operations

By Major Ken M. Woods, Commander, Task Force Raider, JFHQ-C(AF), Team Lead, 403 CMT, Detachment Texas, 782d MI BN (CY)

IN CONTEMPORARY operations, the Army must frequently operate within a Joint environment, collaborating across the service components to achieve tactical, operational and strategic objectives; a facet acutely applicable to Army Cyber units. This article explores a unique perspective and considerations for an Army unit to excel in such interdependent operations. Effective communication, integrated training and exercises, clearly defined roles and missions under a unified command structure, and technological interoperability are all essential components for success. This article delves into the importance of understanding and respecting the unique cultures, capabilities, and operational norms of each service branch, as well as the challenges involved.

Effective communication is the lifeblood of any Joint operation. The operational unit must ensure seamless communication across different service branches and agencies to coordinate efforts, share intelligence, and make informed decisions; a critically important factor during high tempo and high priority missions. Like tinnitus in my infantry ear, this ever-present tone rings true between operational echelons. Clear intent disseminated down, and

reliable, regular updates provided across the Joint force to ensure the end-state is achieved. In addition to communicating the operational campaign across the Joint force, leaders must also communicate down to the team to ensure the operational picture is painted adequately: Sometimes operational tempo dictates painting with your hands, other times one is afforded the time to paint with a fine brush – but that operational picture benefits the team by showing them the efficacy of their labors for their piece of the operational pie. Our Joint operations are accomplished by people, and people are more effective when they know the impact; the “why” and the “so what” behind the campaign. The gravity of this intensifies as sprints so often turn into marathons.

Integrated training and exercises are vital for preparing Army units to operate effectively in a Joint environment. Though an argument can be made for a commander to assume risk, such as validating a team which has proven itself through real world operations under the scrutiny of the “#1 operational priority” mission, it remains an enduring necessity of readiness to continuously evolve and conduct training exercises that reflect Joint operations and attempt to codify a standard of operations. Within our cyber world,

we have a common Joint qualification record for work roles, but our method of utilizing these work roles to accomplish the mission differs between teams and service components. What works well for the Army may not be as effective for the Air Force, and vice versa. But alternative approaches lead to Joint standards. The Army has demonstrated success with finding the “best athlete” within the whole of our government to achieve the commander’s end state – a method not defined in doctrine but widely successful with certain missions. Operating as a Joint force provides opportunity to succeed that is not otherwise as easily achievable from solely a service component perspective.

Clearly defined roles and missions are essential for the efficient execution of Joint operations. Who is the supported command and who is the supporting command? Who owns the mission and who is responsible for ensuring the owner is supported so the mission succeeds? Our service components operate in Joint environments but are not truly Joint. Yet we support and partner with Joint commands. Additionally, though Joint doctrine is necessary and applicable (JP 3-0 or 5-0 is your deskside reading, right?), service doctrine is also relevant and leads to different approaches to planning,

coordinating and executing operations. The Army's approach through the military decision-making process is rooted in ground combat; it is deliberate, thorough, and focused on rapidly achieving the commander's end-state. One of the most significant challenges in Joint operations is understanding and respecting the unique cultures, capabilities, and operational norms of each service branch; and each service branch's cyber component has its own *modus operandi*. At the forefront, and with all the lobotomized bias of being an Army field grade officer, the mindset of effects-driven operations is largely present in the Army culture, with our sister components warming up to adopting and applying this mentality. Acknowledging operational limitations, some sister service combat mission teams (CMTs) would appear to perpetually prepare cyber mission packages without crossing the precipice to executing, while other Army CMTs seem to portray an attitude of "I'm here to do 350-1 and deliver effects, and I'm all green on 350-1." A balance exists

and is found within the Joint force and given time this balance becomes the Joint culture.

Technological interoperability is another cornerstone of successful Joint operations. The Army must ensure that its systems and platforms are compatible with those of other service branches. The pain of turning this simple statement into a reality is not lost on the audience of this article [like Ike]. The reconciliation of the plight of a common operating platform through operational, training, and administrative lanes is neither expeditious nor inexpensive. This quickly leads into the discussion of USCYBERCOMMAND 2.0 and the amelioration of our force and would seemingly require a dissertation to appropriately address but nonetheless is a factor that is imperative to Joint operations. Perhaps that would solve virtual teleconferences (VTCs) across different infrastructure bridges owned by separate commands through multiple classification enclaves. One can dream.

Excelling in joint operations is

non-trivial and requires a holistic approach that encompasses effective communication, integrated training and exercises, clearly defined roles and missions, and technological interoperability. It requires leaders who actively steward these aspects and proactively leverage organizations or best athletes to succeed. It might not be explicitly stated in doctrine, but when has the U.S. military ever really followed doctrine while conducting operations? Rangers, lead the way! One final thought; succeeding in Joint environments requires leaders who can adapt while ensuring their formations do not reach tracer burn-out. *In Army ground operations, tracer burn-out refers to the distance at which the pyrotechnic tracer compound in the round burns and the projectile is no longer visible – allowing a Soldier to rapidly calculate distance (5.56mm burn-out range is 700-900 meters). It's also an infantry idiom for someone who is burnt out due to exhausting work.* ■





Training the Joint Force: How Army processes play an essential role in the Cyberspace Capability Developer (CCD) Work-Role

By CPT Mitchell Stiffler, Cyberspace Capabilities Developer (CCD), D Company, OSE

WHILE UNITED STATES Cyber Command (USCC) outlines required tasks and knowledge, skills, and abilities (KSAs) for progressing to a Senior CCD in this work role's Job Qualification Record (JQR), no standardized process exists across the Military Services. Each Service is responsible for implementing its own pipeline for creating Senior CCDs. Sometimes there isn't even standardization within an individual service. The Army has responded remarkably well to meet this requirement. For each Senior CCD JQR, the Army has a corresponding GitLab training pipeline as well as Senior Skill Level Exams (SSLEs).

The Army has successfully streamlined the process for creating Senior CCDs. This achievement has both given candidates a concrete path for progressing within their work-role and given Senior Leaders a uniform answer to what a Senior CCD is. This success has resulted in Army developers taking up positions of mentorship within the Cyber Mission Force (CMF) CCD community. Members of other services are currently pursuing their Senior CCD qualifications using the Army's pipelines. Army developers are currently mentoring Navy and Air Force developers to help them complete their JQRs and pass their SSLEs. While this program is still in its infancy, it has already had success.

In May of 2024, a Navy developer passed the Army's SSLE for Windows Access. This was the first time a developer from Navy Cyber Warfare Development Group (NCWDG) used the Army's process for becoming a Senior CCD. This certification both contributed to the Navy's readiness and built goodwill between services. As certain Senior CCD specialties lack qualified developers, the

Army may need to call on this goodwill to avoid bottlenecking progression to Senior.

After taking their SSLE, developers must complete a Senior Panel where three developers qualified as Seniors in the applicant's specialty assess the applicant's code and question the applicant's knowledge within that specialty. However, often there are not enough Seniors to fully staff a panel. While there is policy in place to ensure developers can progress when three Seniors are unavailable, it remains a patchwork solution. In cases where a panel can't be staffed by Seniors of the appropriate specialty, a Master developer can sit on the panel. This solution is imperfect both because the Master is not trained in the specialty that they assess the candidate on and because there are very few Master Developers.

The Army can address this imperfection by allowing developers from other services to sit on Senior Panels. This will add resiliency to the senior qualification process by deepening the pool of personnel who are able to sit on a Senior Panel. It will also improve feedback in candidate's SSLEs by introducing Panel Members with unique perspectives gained from working in other Services.

Making this change will also benefit USCC as well. For other Tier One work-roles, the pipeline for mastery is the same. A Master Exploitation Analyst (EA) for the Army completes the same training pipeline as a Master Exploitation Analyst for the Air Force. The same goes for

Interactive-On-Net Operators (IONs). This gives Commanders a straight-forward understanding of the capabilities these work roles provide and how they can be best utilized across their units. Developers stray from this path. The varied pipelines for CCDs give Commanders an inconsistent product. Allowing members

from other Services to sit Army Panels would be a step in the right direction towards creating greater uniformity in the CCD training process. ■

AvengerCon IX returns to the Augusta Georgia Cyber Center



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

AUGUSTA, Ga. – The 780th Military Intelligence Brigade (Cyber) hosted AvengerCon IX, a cyber-con, and the theme was “the intersection of government, industry, and academia in support of advancing cybersecurity,” February 26 and 27 at the Georgia Cyber Innovation & Training Center.

AvengerCon is a free security event hosted by volunteers from the 780th MI BDE to benefit the hackers of the U.S. Cyber Command and Department of Defense. The event is targeted at personnel supporting DoD cyberspace missions, but others are welcome to attend. AvengerCon features presentations, hacker villages, training workshops, and much more (<https://avengercon.com/mission>).

“In military cyber we get a lot of specific pipeline training,” said Army 1st Lt. Andrew White, AvengerCon IX lead organizer and event volunteer. “What we’re kind of lacking is the hacker culture. It’s a little bit harder to do in the military because hacker culture is kind of homegrown, it’s grassroots, it kind of emerges. People aren’t forced to go to hacker conferences.”

Day one of AvengerCon IX was primarily training workshops, and day two began with remarks by the keynote speaker, Dr. Daniel “Rags” Ragsdale, former Deputy Assistant National Cyber Director. Dr. Ragsdale previously served as a Program Manager in the Defense Advanced Research Projects Agency (DARPA) and prior to joining DARPA, Colonel (retired) Ragsdale served 30 years in the U.S. Army in a wide array of operational, educational, and research and development roles.

“We have adversaries of our great nation who are working tirelessly against our interests. The interests of our nation, the interests of the American people,” said Dr. Ragsdale.

“I was commissioned an infantry officer. I was privileged to deploy three different times, but I would tell you that in my mind... everyone in the business and the work that you’re doing is effectively deployed, continuously, and for that you have my great gratitude,” added Dr. Ragsdale. “You are heroes of the current story and the future story. It’s not just about protecting and preserving you’re also part of that integrated deterrence.”

Dr. Ragsdale talked about the early beginnings of Army Cyber in the late 90’s, early 2000’s, when his dissertation chair at West Point asked him to develop a course on information security.

“Armed with this information, and a document, that I will encourage all of you at some point to avail yourselves to, written by two PLA colonels, in the mid-90’s (The People’s Liberation Army is the military of the Chinese Communist Party and the People’s Republic of China), it was called “Unlimited Warfare,” and it was their playbook that they have implemented since that time” said Dr. Ragsdale. “And it was the PLA that said ‘we have no wherewithal to impede, head-on in a military sense with the United States,’ the only superpower at that time. The USSR had dissolved years before. The U.S. was the only superpower, and we have demonstrated some of the capabilities in Desert Storm. They knew they couldn’t compete directly with that, but they aspired to be a superpower. So, what did they do? They look out asymmetrically, outside of direct military confrontation... they looked at financial means to do so, legal means to do so, they didn’t use specific terminology, what can we do in cyber, and they have aggressively pursued a strategy of unlimited warfare with us, surely, at least back to that time.

“I had this document, and I kept it in my office, and I used it to, a vernacular say so, this is what our adversaries are

saying and doing, and here we are at the world’s premiere intellectual, thinking for our Army here at West Point, what are we doing... And I used that document, and I held it up for years and I said what is our response?”

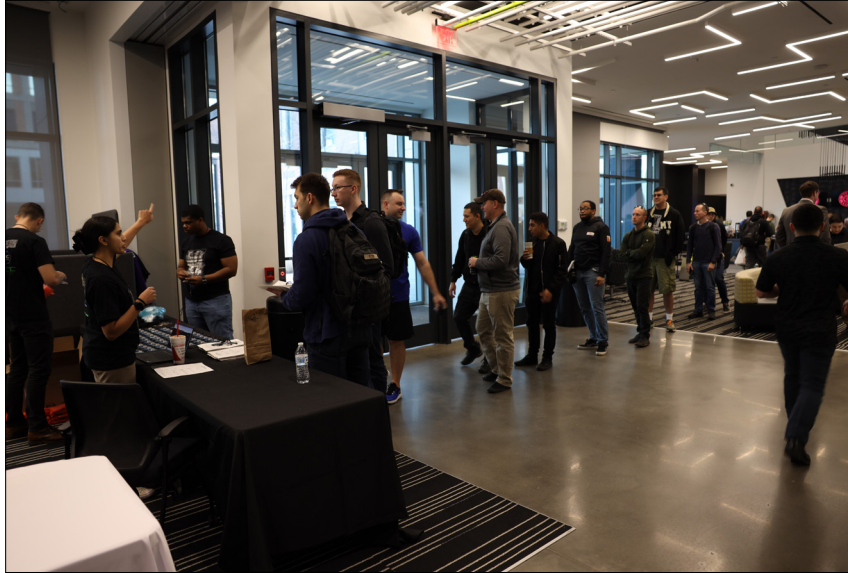
After talking about various topics, including, amongst other things ChatGPT, Large Language Models, and artificial intelligence, Dr. Ragsdale said the biggest take away from his remarks was to “lean into your role as a leader, both as a formal leader and an informal leader.”

He asked the audience, who is on Mount Rushmore, and when someone mentioned Theodore Roosevelt, 26th President of the United States, Dr. Ragsdale said, “Boom! Jefferson and Lincoln, easy. Roosevelt, people like, ‘you know, why is he up there?’ Great man, great man, great man... He said a lot of things that moved me with his words, it’s “In the Arena.”

“Read “In the Arena.” I got goosebumps just thinking about it,” said Dr. Ragsdale. “(Roosevelt) said this and this is the challenge for all of you in terms of both get what you can done but also have strategic patience to know you can’t change everything. He said, ‘Do what you can, with what you have, where you are.’ I want you to write that on your hearts, control what you can control.”

In addition to three-track presentations throughout day two of AvengerCon IX, Chris Thompson, Global Lead of IBM X-Force Red provided the mid-day address; the afternoon panel on Threat Intelligence included Andrew Morris, GreyNoise Intelligence; Michael Grochol, Iron EagleX, and Dr. Sid Stamm, Rose-Hulman Institute of Technology; and Julius Gamble, Regional Director, Cybersecurity and Infrastructure Security Agency (CISA) provided the event’s closing remarks.

In keeping with the AvengerCon IX theme, Gamble said, “True collaboration will best prepare us for the challenges of





of tomorrow. By working together, we can reduce risk and enhance resilience of our nation's critical infrastructure."

The annual cyber-Con has come a long way since AvengerCon started in 2016 as an internal training event hosted by the A Company (Avengers) in the 781st Military Intelligence Battalion at Fort George G. Meade, Maryland (<https://avengercon.com/history>).

"Augusta has been an amazing host to Army Cyber," said Army Capt. Amir Soofi, AvengerCon IX planner and event volunteer. "We could not become who we are without Augusta. It's proximity to Fort Eisenhower, Georgia Tech, Atlanta, an amazing triangle of tech talent here and the outreach we have to the community that is the future of U.S. Cyber. I can't imagine us anywhere but Augusta, it's been an amazing experience."

AvengerCon is a volunteer effort by members of the federal government, in collaboration with Cyber Fusion Innovation Center (CyberFIC), Army Cyber Institute (ACI) at West Point, and Army Cyber Technology & Innovation Center (ArCTIC).

The Soldier volunteers also wanted to recognize the site host, the Georgia Cyber Innovation & Training Center, whom without their support, AvengerCon would not be possible.

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

#Army250 #ArmyCyber #ArmyPossibilities ■





Attracting top talent and building relationships

Army cyber unit's commitment to community engagements and Army recruiting

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

FORT GEORGE G. MEADE, MD. – The Soldiers and Civilians of the 780th Military Intelligence Brigade (Cyber), the Praetorians, embrace opportunities to talk to the American people and support Army outreach and recruiting efforts to inspire (or educate) others to join the United States Army.

The Praetorian Soldiers and Civilians are ideally positioned to assist Army outreach and recruiting efforts as the brigade has a footprint in four U.S. states – Georgia, Hawaii, Maryland, and Texas – and although there are more than 200 ways to serve in the Army, the brigade represents military occupational specialties that most Army recruiters are unable to explain in depth.

From cyberspace operations to electromagnetic warfare specialists; foreign language specialists to signals intelligence voice interceptors; and exploitation analysts to cyber capability developer technicians, the brigade's population of cyber and military intelligence enlisted Soldiers, warrant officers, officers and Civilians represent an array of Army cyber and technology careers (<https://www.goarmy.com/careers-and-jobs/specialty-careers/army-cyber>).

"The Brigade's participation in these engagements is crucial to the growth and development of our unit, as well as the future of our nation's cyber defense," said Col. Candy Boparai, commander of the 780th MI Bde. (Cyber). "By attending these events, we are not only showcasing the Brigade's impressive capabilities and accomplishments but also inspiring and recruiting the next generation of cyber warriors. By sharing our successes and highlighting the importance of our mission, we can attract top talent, build relationships with key stakeholders, and

ultimately contribute to the advancement of our national security."

The 780th MI Bde. is the only operational offensive cyberspace brigade in the U.S. Army and conducts cyberspace operations and capability development to deliver effects in support of Army and Joint requirements (<https://www.linkedin.com/company/780th-military-intelligence-brigade-cyber/>).

In 2024, the brigade's support to the Army's Total Army Involvement in Recruiting (TAIR) spanned from San Francisco to Brooklyn, N.Y., and Las Vegas to Chicago; the Praetorians assist girl scouts in attaining their cyber security badges and host an annual Hackathon for teens – a cyber and computer challenge for young people; the brigade hosts try outs to field Bataan Memorial Death March, Army Ten-Miler, and competitive cyber teams; and hosts an annual AvengerCon at the Georgia Cyber Innovation & Training Center (<https://avengercon.com/>).

"I first learned about the 780th MI Bde. through one of their external engagements – the Army Cyber Skills Challenge," said Lt. Col. Stephen Hudak Jr., a cyber officer and deputy commander of the 780th MI Bde. (Cyber). "If it wasn't for this event, I may not have ended up working in the 780th. This participation allows our brigade to inspire others to join our ranks and expands an understanding of who we are and what we do."

Army Cyber Skills Challenge was a competition organized and staffed by the brigade's warrant officers.

The brigade's Civilian Personnel Office (CPO) attends Army career fairs and select job fairs, including the Scholarship for Service Recruiting Event in Washington, D.C., where the CPO recently extended four tentative job offers for capability developers. To view a current

list of the brigade's open Civilian positions visit: <https://www.usajobs.gov/search/results/?l=&k=780th>.

The U.S. Army offers countless opportunities and offers competitive pay and benefits, including health care, retirement plans and more.

"These engagements are a vital part of our outreach efforts, and we are proud to be able to engage with the community, share our story, and inspire others to join our team," said Boparai.

Did you know:

In 2025, the U.S. Army will proudly commemorate 250 years of distinguished service to our nation, tracing its legacy from June 14, 1775, to the present. The central theme for the birthday and related events "This We'll Defend" highlights the Army's purpose of fighting and winning our nation's wars. It also underscores the Army's commitment to defending our nation's values, security, and people.

#Army250. ■





Vanguard NCO Induction Ceremony

FORT GEORGE G. MEADE, Md. – Command Sergeant Major (CSM) Jermaine Ocean, the senior enlisted leader for the 781st Military Intelligence Battalion (Cyber), Vanguard, hosted a Noncommissioned Officer (NCO) Induction Ceremony to formally recognize and promote 21 enlisted Soldiers to the rank of NCO, in the Fort Meade McGill Training Center Ballroom, February 20.

CSM Ronald V. Krause, the senior enlisted leader for the U. S. Cyber National Mission Force, served as the guest speaker and presented certificates to the new NCOs welcoming them into the NCO Corps.

HOC, 781st MI BN NCO Inductees: SGT Billy Gonzalez; SGT Luke Martin; SGT Brandon Moloney; and SGT William Santiago

A Co, 781st MI BN NCO Inductees: SGT Nicholas Baldschun; SGT Keith Barrow; SGT Niko Butera; SGT Samuel Keehn; SGT Parker Kulczyk; SGT Natalie Lenehan; SGT Matthew McBroom; SGT Sebastian Solberg; SGT Adrian Tovalin; SGT Dujon White; and SGT Logan Williams

B Co, 781st MI BN NCO Inductees: SGT Brian Biggerstaff; SGT Melissa Leusch; SGT Hayden Longo; SGT Carter Pusateri; SGT Adrian Steffen; and SGT Kevin Tran

C Co, 781st MI BN NCO Inductees: CPL Jonathan Villarreal; SGT Jacob Almond; SGT Elizabeth Creek; SGT Curtis McElroy; SGT Johnny Rodriguez; SGT Christopher Sandoval; SGT Shelby Seale; SGT Ian Thomas; SGT William Wilson; and SGT Stoney Wisley
Please join us in recognizing the significant transition of Soldiers to leaders as they join the Army Noncommissioned Officer Corps.
Vanguard... When Others Cannot

#Army250 #ArmyPossibilities #ArmyCyber ■







Cyber Legion NCO Induction Ceremony

FORT EISENHOWER, Ga. – The 782nd Military Intelligence Battalion (Cyber), Cyber Legion, held an NCO Induction Ceremony to induct newly promoted Sergeants into the Army Noncommissioned Officer Corps, January 16, in the Cyber Center of Excellence NCO Academy's Ray D. Lane Room.

The ceremony was hosted by Command Sgt. Maj. Joseph Daniel, the senior enlisted leader for the 780th MI Brigade (Cyber) and Command Sgt. Maj. Kevin Flickinger, the Cyber Regimental Command Sergeant Major, was the guest speaker.

A Co., 782d MI BN NCO Inductees: Sgt. Bryan Arnold; Sgt. Jason Cleary; Sgt. Justin Jackson; Sgt. Nathaniel Jarrell; Sgt. Jayson Nwigwe; Sgt. Ian Shouvlin; Sgt. Alexander Tellez; and Sgt. Noah Trytten

B Co., 782d MI BN NCO Inductees: Sgt. Ethan Lillibridge; Sgt. Gunnar Marshall; Sgt. Keaton Posey; Sgt. John Reber; Sgt. Clayton Walker; and Sgt. Nathan Weak

C Co., 782d MI BN NCO Inductees: Sgt. Laura Frazee; Sgt. Adam Hales; Sgt. Aidan Hillers; Sgt. Nathaniel Peak; Sgt. Pedro Schlatter; Sgt. Lewis Sullivan; Sgt. Jesse West; Staff Sgt. Victor Maysonet

D Co., 782d MI BN NCO Inductees: Sgt. Nolin Bradley; Sgt. Eric Conway; Sgt. Dylan Ditto; and Sgt. Sean Sobik

Please join us in recognizing the significant transition of Soldiers to leaders as they join the Army Noncommissioned Officer Corps. Cyber Legion...Silent Victory

#Army250 #ArmyPossibilities #ArmyCyber ■







Army Brigade Soldier Family Readiness Group (SFRG) Assistant

INTRODUCING MS. LESMES, our new Army Brigade Soldier Family Readiness Group (SFRG) Assistant! Ms. Lesmes serves as a bridge liaison between military families, Soldiers, and the command team, ensuring that everyone has the support and resources they need during deployments, training, and everyday life. Whether you're a spouse, parent, or loved one of a Soldier, you can leverage this position by reaching out with questions, attending SFRG meetings, or volunteering to build a stronger community. Think of the SFRG Assistant as your go-to point of contact for navigating the unique challenges of military life—don't hesitate to connect and take advantage of this invaluable resource!

Family Readiness: "Family Readiness is the state of *being prepared* to effectively navigate the challenges of daily living experienced in the unique context of the Army. A prepared Army Family understands the challenges they may face, is aware of *supportive resources* available to them, has the skills needed to function in the face of challenges, and uses those skills and resources to manage challenges." AR 600-20, Chapter 5

The SFRG Assistant serves as the *champion* of the SFRG membership by:

- Supporting the Command Team's Family Readiness Goals
- Maintaining open communication and relationship with unit leadership, CFRR, SFRSA (if applicable) and Soldier and Family Readiness Advisors
- Completing mission essential activities as outlined within the SFRG SOP and all local policies and procedures
- Working with command team to plan and execute approved SFRG activities
- Ensuring SFRG maintains communication with SFRG membership and provides

information, resources and referrals as needed

- Attending required Family Readiness training and meetings
- Completing required volunteer registration and administrative tasks
- Recruiting and working with all SFRG volunteers

Leyla Lesmes
Family Readiness Support Assistant
780th MI BDE,
Bldg. 310-R Chamberlin Ave.
Ft. Meade, MD 20755
W: (301) 833-6188
DSN: 312 733-6188
leyla.c.lesmes.ctr@army.mil ■



*The FRG is a unit commander's program..." (AR 608-1, J-1a)
"Commanders have an obligation to provide assistance to establish and maintain personal and Family affairs readiness." (AR 600-20, paragraph 5-10)*

Praetorians,
you are cordially invited to attend the
premier gathering of/by/for the American
military cyber community (for free)



*Maintain your certs with continuing education credits
while having a great time with villages, talks,
panels, publications, research, networking,
exhibitors, Mission BBQ, medals, Enlisted Child's
Scholarship, raffles, Cyber Bourbon, colleagues from
across the Joint Force, camaraderie, and much more.*

New Venue: Applied Physics Laboratory, Johns Hopkins University!

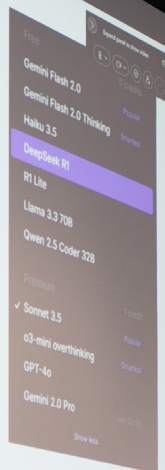
Brought to you by the MCPA, a 501(c)(3) educational nonprofit
charity serving the functions of a regimental style association.

HammerCon.org

What is Websim.ai



- WebSim.AI is a **generative website browser** which was introduced in late March 2024. WebSim.AI is an interactive hub that allows users to create, archive, and share web simulations
- Relies on other AI engines – but packages and makes easily interactable



Current Models Supported



Apex Company, 11th Cyber Battalion Change of Command



FORT EISENHOWER, Ga. – LTC Louis Etienne, commander of the 11th Cyber Battalion hosted a change of command ceremony whereby 1LT Samson Odior relinquished his authority as the commander of Alpha Company (Apex), 11th Cyber Bn., to CPT Guibel Marino, on February 7, at the Fort Eisenhower Conference Center (U.S. Army photos by 1LT Angeline Tritschler).

TRAIN HARD, FIGHT HARD, WIN EASY! GLOBAL REACH, GLOBAL IMPACT!

#Army250



Alpha Company, 11th Cyber Battalion M4 Qualification Range



*Alpha Company, 11th Cyber Battalion successfully executed an M4 qualification range, ensuring all Soldiers met marksmanship standards with precision and discipline. Additionally, the unit conducted M249, M240B, and 50 caliber familiarization ranges, enhancing proficiency and combat readiness across multiple weapon systems. TRAIN HARD, FIGHT HARD, WIN EASY!
#Army250 #ArmyCyber #ArmyPossibilities.*



A Company, 782d MI BN (Cyber) Change of Command



FORT EISENHOWER, Ga. – The officers, noncommissioned officers, Soldiers, and Civilians of the 782nd Military Intelligence Battalion (Cyber), Cyber Legion, bade farewell to Capt. Rachel Martinez, the outgoing commander for A Company, Cyber Archers, 782d MI BN, and welcomed Capt. Jin Lee, the incoming commander, in a ceremony hosted by Lt. Col. Kirklin Kudrna, battalion commander, 782d MI BN, at the Courtyard Pavillion, January 31.

“On Target! Bring ‘Em Down!”

(U.S. Army photos by SSG Torin Marion)



B Company, 781st MI Battalion (Cyber), Change of Command



FORT GEORGE G. MEADE, Md. – LTC Scott Beal, commander of the 781st Military Intelligence Battalion (Cyber), Vanguard, hosted a change of command ceremony whereby CPT James Donahue relinquished his command of B Company (Immortals), 781 MI BN (CY), to 1LT Daniel Alvarado, March 7, at the Fort Meade Post Theater Vanguard...When Others Cannot
#Army250 #ArmyPossibilities)



CONGRATULATIONS!

After a challenging and action-packed week at the ARCYBER/NETCOM Best Squad Competition, the results are in! Congratulations to all the outstanding Soldiers who gave it their all — and a special shoutout to the winners who rose to the top:

- ARCYBER's Best Squad: 11th Cyber Battalion
- ARCYBER's Top NCO: Sgt. Buckwalter, 11th Cyber Battalion
- ARCYBER's Top Soldier: Spc. Robey, 11th Cyber Battalion

Your hard work, dedication, and warrior spirit truly stood out. Well done to all!



Cyber Brigade takes part in Army Information Operations Planners Course

Schofield Barracks, Hawaii – COL Candy Boparai, commander of the 780th Military Intelligence Brigade (Cyber), and CSM Joseph Daniel, the brigade's senior enlisted leader, observed training conducted by the 1st IO Command, April 2.

The course is the Army Information Operations Planners Course and participants included personnel from Detachment Hawaii, 782d MI Battalion (Cyber), 500th MI BDE and 25th Infantry Division.



B Company, 782d MI BN (Cyber) Change of Command



FORT EISENHOWER, Ga. – LTC Kirklin Kudrna, battalion commander, 782d Military Intelligence Battalion (Cyber), Cyber Legion, hosted a change of command ceremony whereby CPT Matthew Last relinquished his command of B Company, Barbarians, to CPT Gun Woo Kim, in front of fellow Soldiers, Family, and friends, at the Eisenhower Lakes Golf Course, March 28.

Cyber Legion...Silent Victory

#Army250 #ArmyCyber #ArmyPossibilities

@U.S. Army Cyber Center of Excellence @Fort Eisenhower @U.S. Army Intelligence and Security Command



Scholarship for Service Recruiting Event



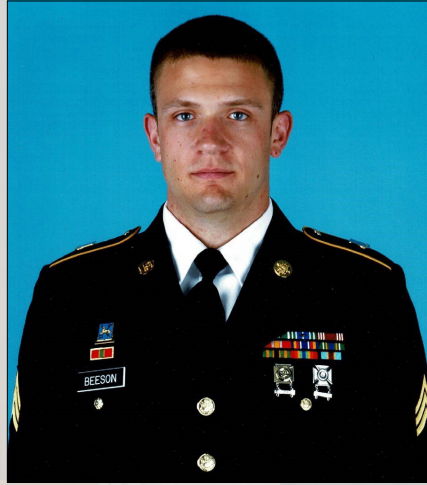
WASHINGTON – The 780th Military Intelligence Brigade (Cyber) was at the Scholarship for Service Recruiting Event in Washington, D.C., January 8 and 9, and the event was so busy these were the only photos... The brigade's Civilian Personnel Office extended four tentative job offers for capability developers. The 780 MI Brigade lists open positions on USAJobs at <https://www.usajobs.gov/search/results/?l=&k=780th>; and also posts these job announcements on their LinkedIn page at <https://www.linkedin.com/company/780th-military-intelligence-brigade-cyber/>.



In Memoriam

SSG Kurtis H. Beeson

781st Military Intelligence Battalion (Cyber)



SSG Kurtis H. Beeson was born one of two children on February 13th, 1992, in Bakersfield, California to Mrs. Lori Riley and Mr. Jeffrey Beeson. SSG Beeson attended various high schools before graduating from Mannheim High School in Mannheim, Germany in 2011.

SSG Beeson enlisted in the Army April of 2011 as 35N Signals Intelligence Analyst. After completion of Basic Combat Training at Fort Leonard Wood, Missouri and Advanced Individual Training at Goodfellow Air Force Base in San Angelo, Texas he was assigned to 3D Military Intelligence Battalion in Camp Humphrey's South Korea as a Signal Intelligence Analyst. After he completed his tour in South Korea, SSG Beeson served as a Signal Intelligence Analyst at Fort Liberty, North Carolina. SSG Beeson arrived at Fort George G. Meade November of 2021 to take on the roles and responsibilities as Target Analyst Reporter for the Cyber National Mission Force. His actions enabled our team to document and disseminate vital information for national defense and the defeat of the nation's adversaries. His work mattered and his actions built a foundation others use to achieve greatness for the nation.

During his service, SSG Beeson was awarded the Joint Service Commendation Medal, Army Commendation Medal Army with three oak leaf clusters, Army Achievement Medal with two oak leaf clusters, Army Good Conduct, National Defense Service Medal, Global War on Terrorism Expeditionary Service Medal, Global War of Terrorism Service Medal, Korea Defense Service Medal, NCO Professional Development Ribbon, Army Service Ribbon, Overseas Service Ribbon, and a Driver and Mechanic's Badge.

SSG Beeson is survived by his parents, mother Lori Riley, father Jeffrey Beeson, and step-father Mike Burrell, his girlfriend, Laura Schwartzmier, and his beloved brothers, Travis Beeson and Vance Fuller.

“...that the impact left by SSG Beeson on all those who knew him is one of everlasting change filled with joy and laughter... His life and story will continue to live on as we remember the best of Kurtis, smiling at the memories just as he would’ve wanted us to.” – CPT Joseph Kim, HOC Commander, 781st Military Intelligence BN

“Those of us who knew Kurtis well understand that he would rather see us have a good laugh together, than mourn his loss. That he would rather see us enjoy fellowship and camaraderie together than shed tears thinking about his memory. That he would rather see the team out on the parade field chasing a frisbee or football together than feeling sad about him being gone. And today, we CAN have that fellowship and camaraderie together, we CAN enjoy that laugh and smile in his memory, we CAN honor him with happiness reflecting on him as these pictures of his incredible life flash on the screen behind me.” – LTC Matt Heinmiller ■





EST.

1775

250



U.S. ARMY

THIS WE'LL DEFEND