780th MILITARY INTELLIGENCE BRIGADE (CYBER)

THE BYTE

Vol. 14, Issue 1

January 2026

THE WARRANT OFFICER EDITION:

Cyber as Maneuver

PRAETORIANS

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.

On the Cover

Hackathon V

ODENTON, Md. – Soldiers and Civilians from Fort George G. Meade hosted the last of the three Hackathon events – a program intended to encourage teen interest in STEM (science, technology, engineering, and mathematics), specifically in cybersecurity – at the Odenton Regional Library, Anne Arundel County Public Library.

Photo by Mass Communication Specialist 3rd Class Jackson Wanous

The brigade's Warrant Officers were responsible for most of the articles and commentaries in this issue of The BYTE magazine.

Chief Warrant Officer 4 Chad Mastbergen, the brigade's command chief warrant officer, established the theme for this issue "Cyber as Manuever."

The theme and articles inside this edition of The BYTE are directly in line with the Army priority to "train as we fight" and all four Army focus areas: warfighting; delivering ready combat formations; strengthening the profession; and continuous transformation.

The 780th Military Intelligence (MI) Brigade (Cyber), and its battalions – the 11th Cyber Battalion, 781 MI Battalion (Cyber), 782d MI Battalion (Cyber), and Operations Support Element – directly support U.S. Cyber Command's core missions: defending the Nation and conducting cyber operations to achieve Combatant Command objectives.

We operate as a key component of the Army's Cyber Mission Force (CMF), specifically providing National Mission Teams (NMT), National Support Teams (NST), Combat Mission Teams (CMT), and Combat Support Teams (CST), and Capability Solutions Developers.

As the Army's only offensive cyber force, the 780th provides unique capabilities to sense, understand, and deliver effects in the information environment globally across tactical, operational, and strategic levels of warfare.

I hope you enjoy these articles as much as I have.

"Ubique Et Semper In Pugna"

"Everywhere and Always…In the Fight!

v/r,
Steve Stover
Public Affairs Officer
780th MI Brigade (Cyber)
Editor, The BYTE

Command Chief Warrant Officer The Byte Introduction

Chief Warrant Officer 4 Chad Mastbergen, Command Chief Warrant Officer, 780th Military Intelligence Brigade (Cyber)

GREETINGS TO ALL, I hope life finds you well. I have been given the opportunity to be the Command Chief Warrant Officer for the 780th Military Intelligence Brigade (Cyber). I am grateful for the opportunity and look forward to serving with and learning from all of you.

Cyber is the newest domain and has been in a constant state of evolution since its inception. The Cyber mission and its forces have been grown to meet the needs of this domain. The Cyber mission forces do not look the same as the mission forces of the other domains. In the Cyber domain you can have a maneuver force that never leaves a sanctuary location just as well as you could have a cyber maneuver force that looks and operates like a traditional force. The cyber mission forces are maneuvering through the digital domains daily, competing against unseen adversaries. Forces in constant contact throughout a cyber battlefield, virtual in some of its construction.

If you look at conflict across the world in the past decades you see "cyber" becoming more of a factor into the evolution of the modern battlefields. Expeditionary cyber will continue to develop in the future. They will be at the digital forefront of the battlefield. Shoot, Move, Communicate, execute the fundamentals to accomplish the tasks given by the commander, remain the same across all domains.

The Brigade will continue to charge forward in helping to shape the cyber mission forces of the future. It will be constantly changing trying to gain the tactical advantages as the adversary and environments develop.

Cyber (OCO, DCO, SIGNAL, and EW) as a Maneuver Force: An Integrated Approach

By Chief Warrant Officer 5 David P. Lucy, Command Chief Warrant Officer, U.S. Army Cyber Command

Introduction

IN THE OPENING HOURS OF MODERN CONFLICT, before the first tank advances or the first missile launches, the battle for the electromagnetic spectrum has already begun. The contest to control cyberspace, communication networks, and the electromagnetic spectrum determines who sees first, who can make more informed decisions, and who has the primary advantage in the early stages of conflict.

In this ever-evolving environment, cyber, signal, and electromagnetic warfare (EW) have emerged as indispensable components of maneuver warfare. When integrated effectively, they amplify a commander's ability to maneuver across the battlefield and fight across all domains. Cyber operations, offensive and defensive, shape the digital terrain by disrupting adversary systems and protecting friendly networks. Signal operations sustain the lifeblood of command and control, ensuring freedom of maneuver through resilient communications. Electromagnetic warfare contests the electromagnetic spectrum itself, denying the enemy the ability to communicate and coordinate with their subordinates.

This article explores how cyber (offensive and defensive), signal, and EW function collectively as maneuver forces, drawing from doctrinal foundations in TC 3-12, FM 3-98, and lessons emerging from the ongoing conflict in Ukraine. The goal is simple but vital: show how their integration transforms CEMA (cyber and electromagnetic activities) from an enabling function into a decisive maneuver element.

Understanding Cyber, Signal, and EW as Maneuver Forces

Offensive Cyber Operations (OCO) are designed to achieve specific military objectives by targeting enemy cyber infrastructure and capabilities. There are three main tenants of OCO: disrupt, degrade, and deny. Disrupting communications is targeting enemy networks to disrupt the flow of information and command and control systems. Degrading is targeting critical infrastructure, such as power grids and transportation systems, to cripple the enemy's operational capabilities. Denying involves limiting or completely removing the enemy's access to their own systems or critical information, creating confusion and delaying their response.

According to TC 3-12, Defensive Cyber Operations (DCO) incorporates information collection, situational understanding, and cyberspace defense. Each of these tasks are essential for protecting friendly cyber capabilities and systems from enemy attacks.

Information Collection and Situational Understanding are defined as defensive cyber forces collecting information and developing situational understanding in cyberspace to understand, shape, and influence the operational environment and consolidate positive gains leading toward desired objectives (4-10). Cyberspace Defense is outlined as the actions taken within protected cyberspace to defeat specific threats that have breached or are threatening to breach cyberspace security measures (JP 3-12).

Signal operation is the management and control of communication networks to ensure the secure and reliable transmission of information. Network management focuses on ensuring the network's capability and function to provide friendly freedom of maneuver in cyberspace. Another aspect of signal operations is deconfliction. This is the coordination that occurs within the cyber scheme of maneuver to resolve issues critical to the effective use and synchronization of signal in a combined arms environment.

Electronic Warfare is comprised of three domains and involves the use of the electromagnetic spectrum to control, exploit, or deny its use by the enemy. Electronic attacks (EA) use electromagnetic energy to attack enemy systems, disrupting their communications and electronic devices. Electronic protection (EP) is defined as guarding/protecting friendly systems from enemy EA, ensuring that critical communications and electronic devices remain operational. Electronic warfare support (ES) is the collection of electronic intelligence (ELINT) to gain insight into enemy capabilities and intentions, enabling more effective targeting and countermeasures.

Coordination and Integration of Cyber, Signal, and EW Forces

Effective cyber, signal, and EW operations require close coordination and integration with other military units. Coordination with Supported Organizations: Cyber, signal, and EW forces must coordinate with supported

organizations to maximize the impact of their operations. This coordination includes deliberate plans to transition any knowledge or capabilities for enduring use and identifying those capabilities which cannot be sustained indefinitely.

Integration and information sharing with Traditional Forces is critical. Cyber, signal, and EW operations must be integrated with traditional military operations to achieve synergistic effects. This involves coordinating cyber-attacks and EW activities with kinetic strikes, electronic warfare, and other military actions. Effective cyber, signal, and EW operations rely on the sharing of information and intelligence. This includes sharing threat intelligence, vulnerability assessments, and situational awareness with other military units and allies.

The application of cyber, signal, and EW forces involves detailed planning and mission thread analysis. Cyber forces can assist in planning by identifying vulnerabilities for future reference by both local operators, regional operators, and cyber forces conducting a defense. Cyber forces assess the defensibility of various components within cyberspace, ensuring that critical assets are protected and that the network can withstand attacks. Cyber, signal, and EW forces analyze mission threads to understand the dependencies and potential points of failure. This analysis helps in identifying critical nodes and developing contingency plans to ensure mission continuity. Engaging Partners and Key Actors: Defensive cyber forces must engage partners and key actors to establish security conditions to defeat threat organizations, shape environments, and consolidate gains.

Cyber-signal operations consist of the simultaneous or synchronized employment of defensive forces to retain the initiative (5-69). Effective cyber-signal operations are built upon relationships, mutual trust, and a common understanding of the operational environment, operation, and mission. They require detailed planning, coordination, and synchronized employment of cyber maneuver and network effects to achieve the commander's objectives and ensure freedom of movement and action (5-113).

Case Study: Ukraine Conflict

The ongoing conflict in Ukraine has provided valuable insights into the effective use of cyber, signal, and EW as maneuver forces. Both Ukraine and Russia have employed a range of cyber and EW tactics to gain an advantage on the battlefield.

Cyber Attacks on Critical Infrastructure: Russia has conducted numerous cyber-attacks on Ukrainian critical infrastructure, including power grids and communication networks. These attacks aim to disrupt essential services and undermine public confidence in the Ukrainian government.

EW Jamming of Communications: Both sides have employed EW jamming to disrupt enemy communications. This has been particularly effective in denying the enemy the ability to coordinate operations and respond to changing battlefield conditions.

Cyber Defense and Resilience: Ukraine has demonstrated remarkable resilience in the face of Russian cyber-attacks. Ukrainian cyber forces have worked closely with international partners to identify and mitigate threats, ensuring the continuity of critical services.

Information Warfare: The conflict has also highlighted the importance of information warfare. Both sides have used social media and other platforms to spread propaganda and disinformation, aiming to influence public opinion and undermine enemy morale.

Lessons from Ukraine for Future Military Operations

The conflict in Ukraine has provided several key lessons for future military operations:

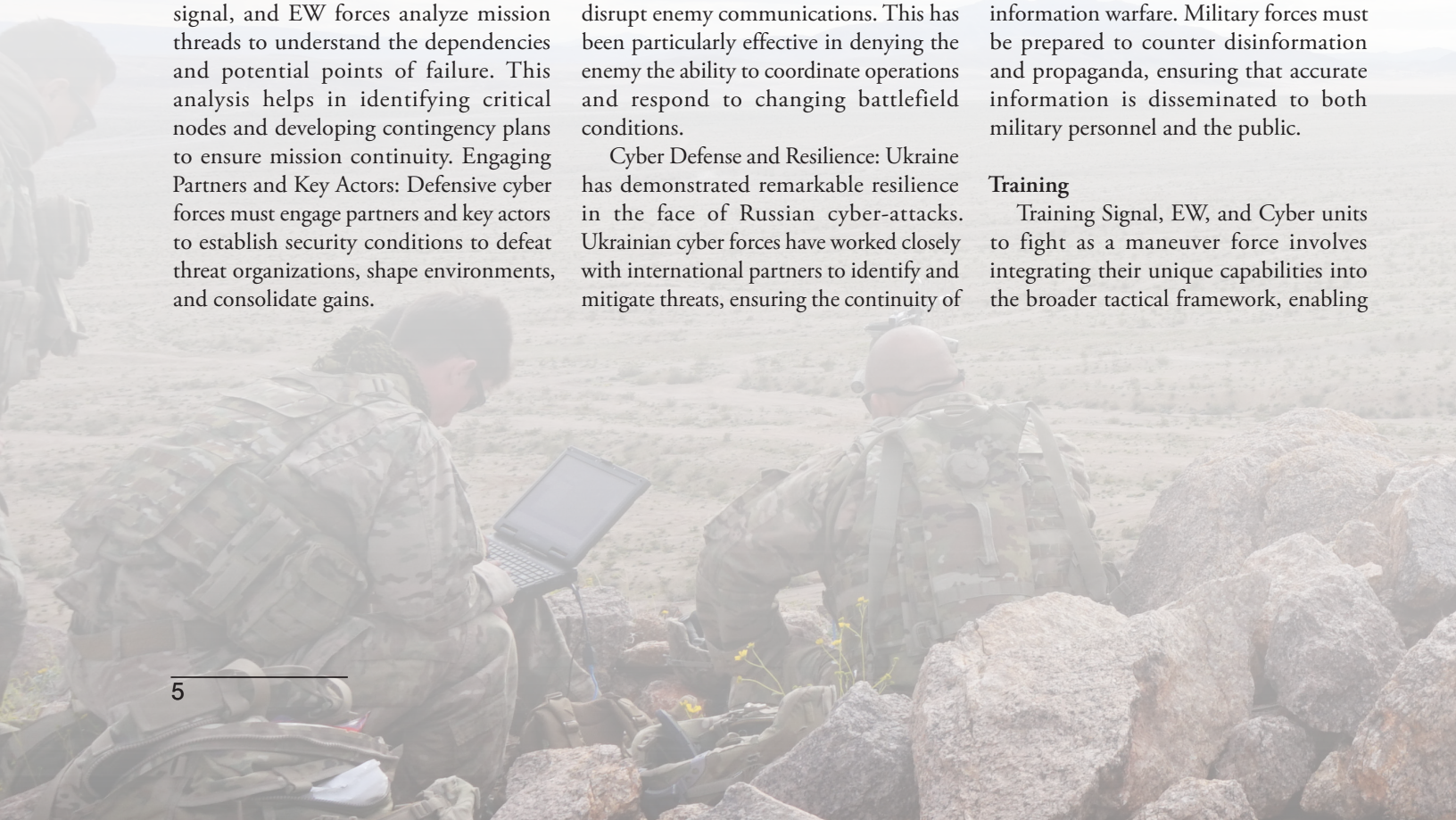
Integration of Cyber, Signal, and EW Capabilities: The conflict has demonstrated the importance of integrating cyber, signal, and EW capabilities into military operations. Effective coordination between these domains and traditional military forces can achieve synergistic effects and enhance overall operational effectiveness.

Resilience and Adaptability: Ukraine's resilience in the face of Russian cyber-attacks highlight the importance of building robust and adaptable cyber defenses. This includes investing in cybersecurity infrastructure, training, and international cooperation.

Information Warfare: The conflict has underscored the significance of information warfare. Military forces must be prepared to counter disinformation and propaganda, ensuring that accurate information is disseminated to both military personnel and the public.

Training

Training Signal, EW, and Cyber units to fight as a maneuver force involves integrating their unique capabilities into the broader tactical framework, enabling



them to support and enhance traditional combat operations. Steps to accomplish this must include the following:

1. Training and Simulation
   - Tabletop Exercises: Use tabletop simulations to plan and rehearse operations.
   - Field Exercises: Conduct live exercises to test and refine tactics.
   - Red Team/Blue Team Exercises: Simulate cyber and electronic attacks to test defensive capabilities.
   - Combined Arms Training: Regularly conduct exercises that involve infantry, armor, artillery, and CEMA units.
   - Scenario-Based Training: Use scenarios that simulate real-world operations to test and refine tactics.

2. Equipment and Technology
   - Advanced Tools: Equip units with the latest cyber and electronic warfare tools
   - Interoperability: Ensure that equipment can communicate and operate seamlessly with other military systems.

3. Doctrine and Tactics Development
   - Doctrinal Guidance: Develop and update doctrines to reflect the integration of Signal and Cyber into maneuver warfare. Incorporate FM 3-12, FM 3-98, TC 3-12_2_98, TC 3-12_2_90, and TC 3-12_2_4 into basic PME for all COHORTS.
   - Tactical Innovation: Encourage innovation and adaptation based on lessons learned from exercises and real-world operations.

4. Leadership and Education
   - Leadership Training: Train leaders to understand and effectively utilize Signal, EW, and Cyber capabilities.
   - Mission-Oriented Training: Ensure that Signal and Cyber units understand their roles in achieving the commander's objectives.
   - Cross-Functional Teams: Create teams that include personnel from Signal, Cyber, and traditional maneuver units to enhance coordination and synchronization
   - Continuous Education: Provide ongoing education and training to keep up with technological advances and evolving threats.

Conclusion

The integration of cyber, signal, and electronic warfare as maneuver forces is a major shift in the way the Army fights. By applying the principles outlined in TC 3-12 and FM 3-98, commanders can synchronize cyberspace, network, and spectrum operations to achieve effects once limited to kinetic fires.

The lessons from Ukraine have proven that digital dominance is just as significant as controlling the physical terrain. The ability to disrupt and defend the cyberspace area of operations and the electromagnetic spectrum is detrimental to the survivability of forces on the ground. It is imperative for our leaders to understand how to integrate CEMA effects into every phase of maneuver, from shaping to consolidation.

As the Army continues to shift to encompass the digital domain, one truth remains clear: future wars will be fought in code and waveforms as much as in mud and metal. Those who fail to maneuver in cyberspace will soon fail to maneuver on land.

The integration of cyber, signal, and EW capabilities into military operations requires a comprehensive understanding of these domains and the ability to leverage data analytics, planning, and mission thread analysis. Cyber, signal, and EW forces must work closely with traditional military units to achieve synergistic effects and ensure the success of operations. The case study of Ukraine illustrates the effective application of these principles, demonstrating how cyber, signal, and EW operations can enhance situational awareness, engage partners, and achieve common objectives.

In conclusion, the concept of cyber, signal, and EW as maneuver forces is a powerful tool in the modern military arsenal. By embracing the principles and TTPs outlined in TC 3-12 and FM 3-98, military forces can leverage cyberspace and the electromagnetic spectrum to gain a strategic advantage, protect friendly assets, and degrade enemy capabilities. The future of military operations will increasingly rely on the effective integration of cyber, signal, and EW capabilities, making it essential for military leaders to understand and implement these principles. The lessons from Ukraine provide valuable insights into the effective use of cyber, signal, and EW as maneuver forces, highlighting the importance of integration, resilience, information warfare, and international cooperation. ■

The Intelligence Warfighting Function as it relates to Cyber. Is it Different?

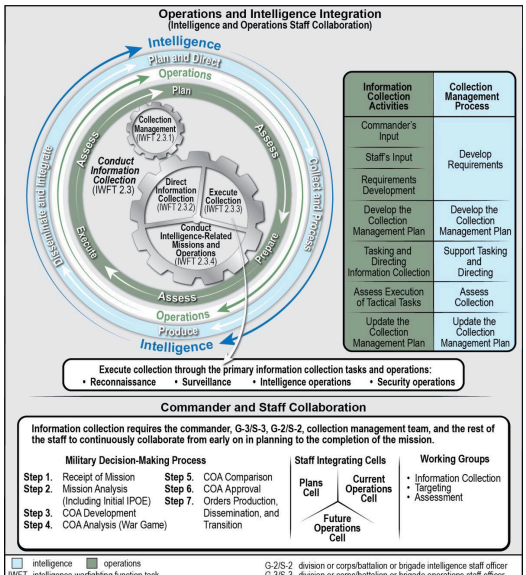
By Chief Warrant Officer 4 Michael Lewis, batallion senior technical advisor, 781st Military Intelligence Battalion (Cyber)

OVER THE YEARS, there seems to be a lot of speculation and rumors about what intel support to cyber looks like. What is in the realm of possible? How does intel support to offensive cyber differ to intel support to defensive cyber? Is it different?

For me, prior to arriving to the 781st in 2021, I had no operational cyber domain experience. Sure, like a lot of folks in this organization, I had some COMPTIA certs and had some college courses in information technology and cybersecurity. Did having those classes matter in the grand scale of intelligence support to cyber? I don't think it did. I believe it helped with learning the vernacular enabling communication with cyber focused people. It helped me understand the nuances of a cyber scheme of maneuver versus a traditional ground component kinetic operation scheme of maneuver. But honestly, I don't believe it really mattered. While intel support to cyber is highly nuanced, I do not believe the nuance is so dramatic that it changes the functions of intel support. When it comes down to it, intelligence provides support to operations, both kinetic and non-kinetic.

What is the Intelligence Warfighting function? FM 2-0 (Intelligence), paragraph 1-21 states, "Intelligence is one of the warfighting functions that enables the Army to generate combat power during the conduct of operations. The *intelligence warfighting function* is the related tasks and systems that facilitate understanding the enemy, terrain, weather, civil considerations, and other significant aspects of the operational environment." During my time as a 35N/352N, having supported Tactical, Operational and Strategic level operations, I can attest the Intelligence Warfighting Function does not change no matter the echelon or type of mission it applies to. Each mission is nuanced. That nuance is based upon the Commander's requirements and end-state of the mission. This is the foundation of intel support.

If you look at Cyber as maneuver, the same foundation applies. I like to say, "Cyber is a tactical action arm with strategic level effects." It requires deliberate planning at strategic and operational levels to identify legitimate end goals. You must understand the operational environment, identify gaps, conduct collection management, collect, process, analyze, and disseminate information to support the operation. To do this, it requires deliberate planning at strategic and operational levels and coordination, collaboration, and constant communication between the S/G/J-2 and the S/G/J-3 to ensure the mission is in line with current approved authorities and meets the commander's intent.



The above graphic from FM 2-0 highlights what collaboration would look like between the intelligence process and S/G/J-2 and the S/G/J-3 agnostic of the type of effect the mission is working to accomplish.

The intelligence warfighting function starts with "plan and direct." This requires commander's input in the form of requirements and orders. From a staff perspective, this function is where the Commander's Priority Intelligence Requirements (PIR) are developed and approved. This will drive collection management and separate mission elements to conduct further coordination and planning to request information and decide how to delegate tasks to complete the process. From the Intelligence Analyst perspective, you take commands from the tower and work to conduct the intelligence process (Collect and Process, Produce, Disseminate and Integrate). It is the integration of the intelligence you produce which will answer the commander's PIRs. It takes the collective actions of individual analysts, teams, and staff, utilizing the existing intelligence warfighting functions, ensure successful mission operation.

Overall, while some tend to believe cyber is new, it has been around for a while. The processes which enable successful operational mission execution has also been around for a while. Intelligence exists to answer requirements which enables operations. Successful intelligence support to cyber falls in the hands of leaders, at all levels, to understand and integrate the intelligence warfighting function into operations throughout the entirety of mission planning AND throughout the entirety of mission execution. It should not be an afterthought or justification for an operation. Cyber leaders which understand how to incorporate this function early will have more successful and arguably more impactful operations in the future.

What Junior Soldiers Expect from Warrant Officers: Building the Future of the Cyber Corps

By Spc. Charles J. Shimazaki, 17C Cyber Operations Specialist, 781st MI Battalion (Cyber)

AS A JUNIOR ENLISTED SOLDIER IN THE U.S. ARMY CYBER CORPS, I have come to understand that technical excellence alone does not sustain our superiority in the cyber domain; it is the deliberate knowledge-transfer of cultivated knowledge, mentorship, and leadership that ensures our continued dominance. Warrant Officers, our subject matter experts and technical leaders, play a pivotal role in this process. Their mentorship is not just appreciated; it is essential.

The Cyber Corps is unlike any other branch. The skills and know-hows developed here are not interchangeable with civilian IT or cybersecurity roles; they are tailored to the unique demands of military operations, national defense, and mission assurance. These capabilities are forged through years of experience, trial and error, and operational exposure. They cannot be replicated by reading manuals or watching tutorials; they must be passed down through mentorship and hands-on development.

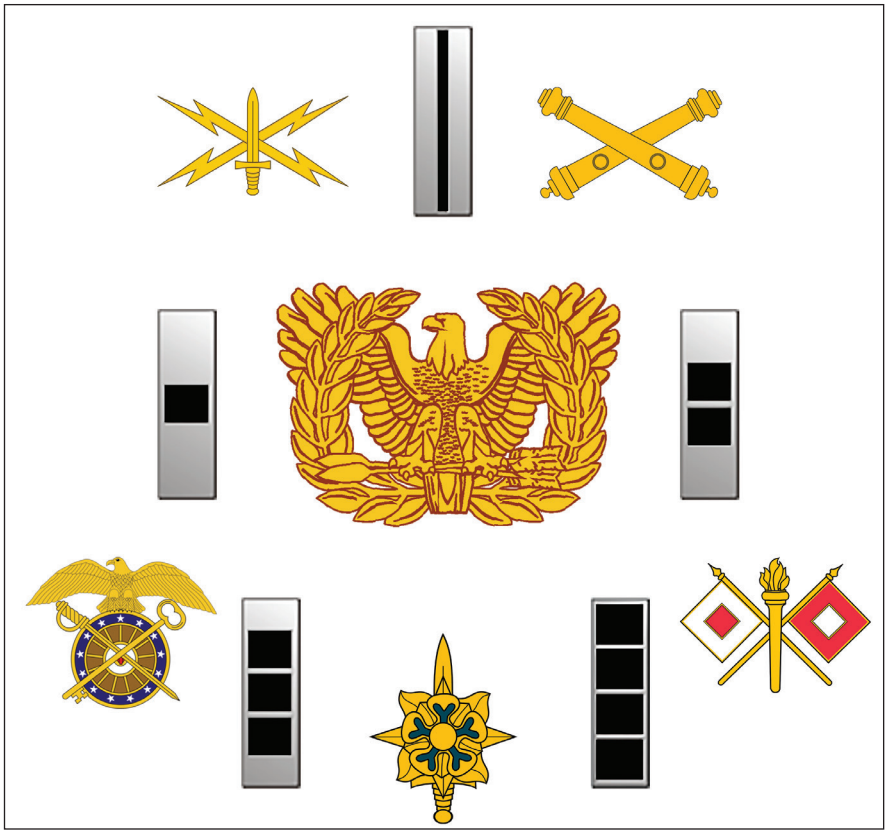
Warrant Officers are the stewards of this institutional knowledge. Their ability to mentor junior soldiers, to explain not just the "what" but the "why" and "how", is what transforms a technician into a tactician. When a Warrant Officer takes the time to share lessons learned, operational insights, and strategic thinking, they are not just teaching a skill; they are investing in the Army's future. One day, every leader must retire; if their knowledge is not transferred, their legacy risks being lost.

History offers cautionary tales. Consider the case of a major technology corporation that failed to document and transfer its proprietary systems knowledge before a wave of retirements. The result was catastrophic; systems failed, productivity plummeted, and millions were lost in recovery efforts. The company had the talent but lacked the foresight to prepare successors. In the Army, such a lapse could mean mission failure or compromised national security.

Junior soldiers look to Warrant Officers not just for answers, but for development. We seek opportunities to shadow, to be challenged, and to be trusted with responsibility. We value constructive feedback and the chance to learn from real-world scenarios. When Warrant Officers engage with us, when they take the time to mentor and develop, we grow faster, perform better, and become more capable of stepping into leadership roles ourselves.

Respectfully, we understand that Warrant Officers carry immense responsibilities; their time is limited and their tasks are complex. Yet, the investment they make in junior soldiers pays dividends. It strengthens the Corps, preserves critical knowledge, and ensures continuity of excellence. Mentorship is not a distraction from the mission; it is a force multiplier.

The Army Cyber Corps must remain at the apex of the Cyber domain. That requires more than cutting-edge tools; it demands a culture of mentorship, knowledge sharing, and deliberate development. As junior soldiers, we are ready to learn, eager to contribute, and committed to carrying the torch. With the guidance of our Warrant Officers, we will be prepared to lead when the time comes. ■




THE EXPERT'S GHOST
IMPOSTOR SYNDROME IN CYBER

The Expert's Ghost: Why Impostor Syndrome Never Leaves in Cyber (And What We Do About It)

By Chief Warrant Officer 3 Arsenio Pagan, 781st MI Battalion (Cyber)

NO MATTER WHERE YOU ARE IN YOUR CAREER, self-doubt is always hanging out on your shoulder. Here I am 17 years in, and the imposter syndrome continues to present itself. In our career field, the room is always jam packed with talent at all levels. As with all things, there is always something new and there is always new experience to gain. Let's dig into why our field is a perfect incubator for imposter syndrome and what we can do to fight it, from the senior leadership's office to our own keyboards.

The "Why Cyber" Dilemma

The "Why Cyber" dilemma stems from the massive scope of knowledge required for our roles, compounded by a high-stakes environment that adds stress to everything we do. It's common to walk into a new role and immediately feel like you're back at square one. The added pressure of already being considered an expert can set expectations sky-high, creating a gap between perception and reality.

When I transitioned from Defense to Offense five years ago, I felt like I was brand new to the exact same career field. Suddenly, asking questions and trying to figure things out felt daunting. This environment, where technology changes almost weekly, is a perfect incubator for self-doubt. And this pressure doesn't just impact newcomers; it creates a unique paradox for the most experienced among us.

The Senior Angle

For senior practitioners, the relentless pressure of a cyber career doesn't fade with experience—it often gets worse precisely because "you're the expert."

As a Warrant Officer, we are designated as the technical experts, relied on to teach and mentor everyone on our teams. The expectation is that you are the SME, period. No one sees the "less than two years" you might have in a specific cyber domain; they see the "15 plus years" of military or professional experience on your resume. This can be paralyzing. It's the expert's paradox: the more you learn, the more you become aware of how much you don't know, all while the expectations from others continue to climb.

The Leader's Responsibility

This environment creates a critical and immediate responsibility for leadership. Given the high stakes, leaders must actively work to counteract this pressure, yet many dont know how. It's not always their fault—the field is complex, with countless moving parts and reporting channels.

However, leaders must bridge this gap. Instead of managing from a distance, they need to engage with their subordinates and work alongside them to understand the daily pressures they face. The mental toll of this field is unique. We need a "Leader's Playbook" focused on building psychological safety, where the mindset shifts from reprimand to lessons learned.

This means creating a culture where subordinates can admit to mistakes or knowledge gaps without fear of reprisal. It's a team where a junior analyst can say "I don't know" and a senior can reply, "Neither do I. Let's find out together."

A Practical Toolkit

While leadership can fix the environment, we must manage our own minds. These are the day-to-day strategies to fight back against self-doubt and build a resilient career.

- ***Embrace "I Don't Know."*** Remain teachable and don't let pride get in the way. The most respected experts are not the ones who know everything, but the ones who are the most curious and resourceful. Reframe "I don't know" as the start of a new discovery, not the end of your credibility.
- ***Be a "Resource Expert."*** You don't have to be the source of all answers, but you should be the person who knows how to get them. Find the experts in the field and know who to ask and when to ask. This isn't a weakness; it's a critical leadership and senior-level skill. Building this network is a strategic objective.
- ***Keep a "Win" File.*** Imposter syndrome is a feeling, and the best way to fight a feeling is with facts. Create a folder labeled "Wins," "Kudos," or "Accomplishments." When you get a "thank you" email, a "good job" from a boss, or successfully close a project, save it there. When you feel like a fraud, go read your facts.
- ***Teach What You Know.*** The fastest way to realize how much you know is to teach it to someone else. Mentor a junior analyst, write a blog post, or lead a lunch-and-learn. Being forced to articulate a complex topic from start to finish will solidify your own expertise and demonstrate your value in a tangible way.

Conclusion

The expert's ghost will probably always be on our shoulder, but it doesn't have to be in the driver's seat. By building safer cultures and practicing individual resilience, we can turn that voice of doubt into a motivator for humility and a driver for the lifelong learning that defines our field. ■

Cyber as Maneuver: A Perspective from Experience

By Chief Warrant Officer 2 Young B. Lee, SIGINT Analysis Tech, 782nd Military Intelligence Battalion (Cyber)

AT OVER 50 YEARS OLD, with more than a decade as a 35P SIGINT (Signals Intelligence) Voice Interceptor and only two years since transitioning into a 352N Signal Intelligence Analysis Technician, my journey to becoming a newly sworn-in Chief Warrant Officer 2 has been anything but conventional. The learning curve has been steep, especially stepping into the fast-moving world of cyber operations. Every day brings new concepts, tools, and terminology; often more than I can comfortably digest. Yet experience has taught me that real learning is not defined by speed, but by the mindset with which we approach understanding, particularly in a domain as complex and rapidly evolving as cyberspace.

When I first arrived (PCS'd) to the 502nd Cyber Support Team (CST), it felt like entering a different universe. Despite 10 years of SIGINT experience, the cyber environment presented challenges unlike anything I had encountered before. I had heard the phrase "Cyber as Maneuver," but initially struggled to grasp its true meaning. In the SIGINT community, we focused on how information flows across the battlefield and how exploiting that flow provides advantage. Translating that same logic into the cyberspace domain required a shift in thinking that wasn't immediate or intuitive.

At its core, "Cyber as Maneuver" is about using the digital environment to seize and maintain positional advantage over adversaries. In traditional maneuver warfare, we think of forces moving across physical terrain to outmaneuver the enemy. In cyberspace, that maneuver occurs in the virtual realm. ADP 3-0 defines maneuver as gaining and retaining the initiative, and in the cyber domain we do this by influencing, disrupting, degrading, or denying an adversary's access to critical systems. It is a contest over information, control, and the integrity of networks.

Early on, however, the cyber domain felt like an overwhelming blur of acronyms, tools, and technical jargon. Even with my background as a 352N accustomed to signal analysis, I struggled to draw parallels between SIGINT operations and cyber maneuver. The more I tried to absorb concepts, the more difficult the learning process felt. But through training, education, and reflection, the principles behind "Cyber as Maneuver" gradually came into focus.

One of the most important realizations I have gained is that cyber maneuver is not primarily about speed. Instead, it is about perspective; the ability to see the larger operational picture and understand how cyber effects shape the mission environment. Over the course of my career, both in SIGINT and now in cyber, I have learned that strategic thinking matters far more than how quickly we can execute a task. What counts is understanding the "why" behind each action and ensuring decisions are made with intent and foresight.

The true power of "Cyber as Maneuver" lies in its capacity to influence the adversary's decision-making process. While traditional warfare contests physical terrain, cyber warfare contests digital space: information pathways, system integrity, and network infrastructure. Cyber capabilities allow us to disrupt communications, degrade systems, and deny access in ways that may be invisible to the enemy but profoundly alter the operational environment.

ADP 2-0 reminds us that intelligence is valuable not merely when collected, but when acted upon to generate effects. Cyber operations represent the seamless meeting point between intelligence and action. Instead of only intercepting signals, we now possess the means to manipulate systems and shape adversary behavior directly. In this way, Cyber as Maneuver becomes a true force multiplier.

In conclusion, mastering cyber mission is not about learning every tool or technique; it is about embracing tempo, acting faster and more intelligently than the adversary, and maintaining digital initiative. For someone coming from a SIGINT background, the real transition is not one of technical skill alone, but of mindset: adapting to the rhythm of cyberspace while holding firm to the principles that guide our service. ■

Cyber as Maneuver (The New High Ground)

By Chief Warrant Officer 2 Quincy-James Julian, Detachment Hawaii, 782d MI Battalion (Cyber)

Rethinking the Battlefield in the Fifth Domain

THE BATTLEFIELD IS NO LONGER DEFINED SOLELY BY LAND, AIR, SEA, OR SPACE – cyberspace has become the fifth domain on the battlefield. A terrain that is regularly contested even more so in today's operations. Sadly, cyber operations are often delegated to support: defending networks, collecting intelligence, or enabling other units. That perception must change. Cyber is not just support; it is maneuver, and treating it as such can decisively shape the fight.

Digital Terrain and Maneuver

Maneuver, in military doctrine, is moving and positioning forces to gain advantage. When I think of maneuver on the battlefield, I picture infantry Soldiers bounding and flanking the enemy, tanks getting in position for the critical shot, and Humvees zooming down the terrain to assist. In cyberspace, the terrain is data, networks, and access points. Flanks are unpatched systems, insecure endpoints, and latent vulnerabilities. Movement is digital, effects cognitive, and tempo is measured in milliseconds.

Cyber maneuver can achieve and have kinetic effects on operations. Suppressing an enemy's integrated air defense system through network denial can achieve the same operational objective as artillery with greater precision and lower risk. Disrupting logistics or command-and-control systems can stop enemy forces in their tracks, creating windows for physical maneuver. Exercises have shown cyber effects directly influence tempo, maneuver, and operational outcomes.

The Warrant Officer Role

Warrant officers bridge doctrine and execution. We are able to translate the commanders intent into technical plans and ensure cyber is fully integrated into operations. Cyber maneuver requires deliberate planning, coordination, and synchronization with physical forces. Leaders must understand that cyberspace is also a crucial terrain to seize, hold, or deny.

In multi-domain operations, cyber effects can reduce risk, create critical operational windows, and enhance maneuver operations of ground forces on the battlefield. Recognizing cyberspace as maneuver space is essential. Warrant officers assist teams with the integration, ensuring that digital effects are intentional, synchronized, and decisive. Cyber is the new high ground and it's time the Army fights for it.

The Keyboard as a Weapon (Tactical Cyber Maneuver)

Maneuver Beyond the Physical

When soldiers or anyone really, thinks of maneuver, they picture mechanized armored formations or infantry squad/team assaults. I was once one of those persons, but now I think in terms of keystrokes. In cyberspace, what maneuver means to me is moving through networks, exploiting vulnerabilities, and shaping the operational environment to gain decisive advantage. While it may lack the big booms and bangs of traditional combat, cyber maneuver can produce devastating effects on the enemy maybe even rivaling kinetic operations.

Reconnaissance and Timing

Cyber operations just like other types of operations, begin with reconnaissance. Traditional cavalry scouts map terrain and become an early warning system of enemy movement. The same can be said for cyber teams. They map networks, identify choke points, and detect adversary presence. Once the battlefield is understood, maneuver is planned. Precise lateral movement through systems, gaining privilege escalation, and placing digital effects. Timing, placement, and context is critical, milliseconds and a certain key being pressed can determine success or exposure.

Integration with Physical Maneuver

Cyber effects should synchronize with physical operations. Disrupting enemy command-and-control, degrading enemy targeting feeds, or delaying enemy logistics enables brigades to advance faster, safer, and more decisively. Cyber operations, if used in synchronization with physical operations, can be force multipliers, complementing or directly influencing tempo and outcomes.

Warrant officers are the bridge between tactical intent and technical execution. We advise commanders and translate objectives into actionable cyber plans, and become the glue that holds everything together across domains. Success requires both mastery of maneuver doctrine and technical expertise.

The future battlefield will be defined by simultaneous movement in physical and digital domains. Cyber operations give us opportunities to fix, deceive, and dominate the enemy before physical contact. "Cyber as maneuver" is no longer theoretical; it happens every day. Warrant officers lead the charge, ensuring digital effects are decisive. ■

Cyber as a Maneuver: Enabling Freedom of Action Across the Modern Battlefield

By Warrant Officer Jessica Mojicamota, 170B, Electromagnetic Warfare Technician, 11th Cyber Battalion

MODERN WARFARE ISN'T LIMITED TO TANKS, INFANTRY, AND AIRCRAFT MOVING ACROSS PHYSICAL TERRAIN. Today, the Army recognizes cyberspace as a battlefield, just as land, air, maritime, and space. Army doctrine identifies that commanders must integrate cyberspace and electromagnetic activities to maintain freedom of maneuver in the digital domain while denying the enemy the same advantage. In simple terms, "cyber as a maneuver" means using cyber capabilities to move, fight, and gain the upper hand in the digital battlespace just as Soldiers would maneuver on physical terrain. JP 3-12 (Cyberspace Operations) supports this by defining cyberspace operations as actions used to achieve military objectives in or through cyberspace, making cyber a true combat capability, not just a support function.

In hopes that junior Soldiers are reading these articles, the easiest way to understand cyber maneuver is to compare it to clearing a building. Before kicking in doors, a squad may cut power or jam enemy radios so they can't see or communicate. Cyber effects accomplish similar actions, except they can do it remotely by shutting down security systems, blocking communications, disrupting enemy sensors, or feeding false information to confuse the enemy. Just like suppressing fire enables a squad to bound forward safely, cyber effects create space for maneuver forces by blinding, confusing, or slowing an enemy before friendly forces arrive. Cyber doesn't replace Soldiers on the ground, it helps them move with less risk and more precision.

On the modern battlefield, cyber maneuver happens alongside kinetic action. Before an air assault, artillery fire mission, or armored breach, cyber Soldiers may deny enemy access to early warning systems, disrupt enemy C2, disable air defense radars, or interfere with reconnaissance drone. These effects provide commanders with a positional advantage, enabling friendly forces to enter contested areas faster and with reduced exposure. FM 3-12 (Cyberspace Operations and Electromagnetic Warfare) emphasizes this synchronization by integrating CEMA across warfighting functions to maximize complementary effects in and through cyberspace and the electromagnetic spectrum (EMS). Cyber is not isolated in a server room. It is a maneuver tool used alongside fires, intelligence and ground forces.

Cyber maneuver matters to every Soldier, not just those in a SCIF or working behind a keyboard. Protecting radios and networks ensures units can call for fire and MEDEVAC without interference. Securing mission command systems ensure orders reach the front lines. Disrupting enemy GPS protects friendly vehicles and aircraft from navigation interference. Denying enemy drone operations protects patrols, convoys, and battle positions from surveillance. Even stopping enemy propaganda or false information online protects community morale and prevents confusion amongst the population. Every Soldier who relies on communications, GPS, drone, mission planning software, digital maps, or battlefield networks benefits directly from cyber maneuver.

The terrain in cyberspace may look different, but the principles of maneuver remain the same. Instead of seizing hills or bridges, cyber forces fight for access to servers, routers, networks, GPS signals, satellite links, power systems, and information platforms. JP 3-0 (Joint Operations) explains that future fights demand integration across all domains, meaning a Soldier at a terminal may create the advantage a Soldier with a rifle needs on the ground. In many cases, digital access becomes the key terrain that determines who can shoot, move, and communicate first, and who cannot operate at all.

Ultimately, "cyber as a maneuver" means treating the digital realm like any other battlespace using cyber effects to out-position, out-pace, and out-fight the enemy. Cyber and conventional units must work together to shape the battlefield, protect friendly systems, disrupt enemy capabilities, and create opportunities for our armed forces to dominate. In future conflicts, victory will go to the side that can move fastest not only physically, but digitally. By integrating cyber into maneuver planning at every echelon, from junior Soldiers securing radios to strategic-level offensive cyber operations, the Army ensures it can fight, survive, and win in a world where data, networks, and information are as decisive as bullets and armor.

The Fifth Domain: Cyber as a Force Multiplier

By Warrant Officer Willem Brunner, Operations Support Element

Cyberspace has emerged as the newest domain of conflict, promising unprecedented opportunities and daunting challenges. Advocates still imagine cyber operations as decisive tools capable of crippling nations before a single shot can be fired. In reality, cyber operations have proven far more complex. They are disruptive, costly, and challenging to scale, yet consistently powerful in assisting traditional military tactics, techniques, and procedures. Rather than replacing tanks, aircraft, or soldiers, cyber has emerged as a force multiplier — expanding the fog of war and enabling intelligence. At the same time, its potential for direct, decisive effects remains unrealized.

The fog of war describes the uncertainty and risk inherent in combat. Cyber represents an expansion of this concept, extending it to the reliability of equipment and networks from tactical to strategic levels. While theorists have long speculated that offensive cyber operations could shape battles, in practice, this has rarely occurred. Over the past two decades, cyber has been employed, but it has yet to be used in tandem with physical effects in a way that decisively alters combat. A notable case is the ongoing Russo-Ukrainian War, where Russia has used DDoS (Distributed Denial-of-Service) attacks primarily for disruption (among other methods discussed later). Yet these efforts have not proven decisive; the outcome of the war continues to hinge on conventional military power rather than cyber operations.

Offensive cyber operations can pursue many objectives — to deny, degrade, disrupt, destroy, or manipulate — yet none have been achieved on a grand scale. Is this because the goals themselves are too limited, or because the feat is simply insurmountable? Unlike conventional weapons, cyber-attacks lack a tangible form but still require significant investment to design and deploy. Their payoff, however, is uncertain; a successful strike may cause disruption but rarely guarantees a decisive advantage. By contrast, defensive cyber operations offer a continual return: every attack repelled is a measurable success, visible in real time. Still, in the broader calculus of war, can the safer option alone ever prevail?

The most consistently employed offensive cyberattack by nation-state actors has been the DDoS attack. One could also argue that Russia's misinformation campaigns during the Russo-Ukrainian conflict fall within the offensive cyber spectrum. Yet across recent conflicts, cyber operations have functioned more as combat enablers than decisive finishers. Attacks on U.S. infrastructure in recent years illustrate the potential for disruption and, in theory, could cause significant damage. However, without a highly coordinated, multi-targeted campaign, such strikes are unlikely to bring about systemic collapse. In this sense, cyber-attacks on critical infrastructure resemble the German bombings of Britain in WWII: both generated disruption and fear but ultimately failed to break national resolve or decisively end the conflict.

Early advocates of cyber warfare envisioned it as a tool capable of ending wars before they began — routing an adversary without ever setting foot on foreign soil. While such a sweeping victory remains theoretically possible, no conflict to date has witnessed a cyber-attack of that magnitude. Instead, modern wars have demonstrated the opposite trend: smaller, more consistent operations are favored, and increasingly resilient defenses make large-scale strikes less likely to succeed.

The most consistently practical application of cyber has been in intelligence. Unlike offensive strikes, intelligence operations are easier to quantify, control, and integrate with other domains. The information they provide enhances decision-making, empowers conventional forces, and delivers tangible results without drifting into theoretical speculation. In this way, cyber finds its strongest role not as a war-ending weapon, but as a force multiplier that sharpens the effectiveness of traditional military power.

Cyber warfare has matured, but its role remains more limited than imagined. Offensive operations have proven disruptive but have been unable to deliver decisive battlefield outcomes. Defensive measures, by contrast, provide continual value, and intelligence stands out as cybers most reliable and enduring contribution. In modern conflicts, offensive cyber operations have not created decisive victories. Instead, cyber acts as a force multiplier — expanding uncertainty, enabling intelligence, and supporting traditional military power. The vision of cyber delivering decisive, war-ending strikes remains unrealized and increasingly unlikely. Cybers value is realized as a vital domain within multi-domain operations, amplifying the effectiveness of the joint force.

My Family and the History of the NCO Corps

By Staff Sgt. Mason Showalter, Exploitation Analyst, 781st Military Intelligence Battalion (Cyber)

ON SEPTEMBER 18TH OF THIS YEAR, I had the privilege of briefing the History of the Non-Commissioned Officer Corps at Valley Forge in front of the monument dedicated to the father of it, Baron Friedrich von Steuben. I gave this presentation through the lens of my own family's history, as my lineage is full of men who didn't have the sense to go to college and who have served during some of the most transformational wars that shaped the NCO Corps. In this article, I will be reformatting that oral brief to paper as well as providing some meta narrative on the thoughts and feelings I had preparing to give said brief, and how it felt to visit the land where my forefather had suffered that long winter in 1778 that tested and defined America's earliest leaders.

My six-times great grandfather, Daniel Schrodenwaller, was an immigrant from Germany, coming to America on the U.S.S. Brotherhood in 1774. Thankfully for me, after stepping off the boat he took the opportunity to "Americanize" his name down to Showalter when signing the boats ledger. There's little I can say definitively about the man himself, now 250 years removed. Everything I know of him comes from a collection of scrapbooks that had been meticulously maintained and passed down through my family for generations. As the most current Soldier in our history, the responsibility falls squarely to me. I wish I could know more about the man himself, but I do know demonstrably that the man had grit.

Shortly after the "shot heard 'round the world", him and thousands of others of soon to be American men were galvanized into joining the Continental Army. However, at this point, it was less of an Army and more of a militia. They were farmers, blacksmiths, and the occasional drunkard. General Washington knew that to have any chance of defeating the British, and winning the war, he'd need to transform these men into a capable fighting force. To accomplish this, he enlisted the help of someone who had himself made that transition from commoner to decorated military officer, Baron Friedrich von Steuben.

Von Steuben quickly set out to work and created a model company of 120 men. He'd stay up at night writing drills, and then spend the day teaching them. Once these men managed to impress him, he scattered them throughout the force to train the others. These 120 men were the first of the Non-Commissioned Officer Corps. Corporals were the primary trainers, Sergeants led men during battles, First Sergeants managed the health and welfare of all men in the Regiment and provided the commander the status of the Troops each morning (A tradition that those of you familiar with a PERSTAT are still well aware of). Sergeant Majors were the senior advisors to Regimental Commanders and handled various matters of unit administration and record keeping. It is thanks to their efforts especially that I can tell you today that Daniel Schrodenwaller was a Corporal at Valley Forge.

However, one key responsibility applied to every NCO. A mandate to maintain good order and discipline. The groundwork laid by von Steuben made clear the chain of command, and gave a common language for officers to communicate with NCOs. The outcome of all of this is that the commoners became a fighting force fit to rival the second largest standing army in the world. America earned its independence through brave men and women from all walks of life.

I'd feel remiss if I didn't mention here what I didn't know when preparing the oral version of this presentation. The continental Army wasn't just composed of the men I'd saw in paintings and history book pictures growing up, 10 percent of the Soldiers at Valley Forge during that harsh winter were people of color. From the earliest battles our country ever fought, men and women of color were there, fighting for the idea of America. Where all men are created equal, and all people have unalienable rights. For them, the fight for America was a fight to sever both a political bondage and a literal, far more personal one. There are many lessons we can take from the Revolutionary War, but one that is seldom reiterated is the importance of immigrants, women, and people of color in securing this nation's independence. During the staff ride, one of 781st MI Battalion's very own, Fred Robbins, briefed the history of these overlooked Patriots and their contributions to winning the war that allowed him and I to wear the Uniform and fly the flag we love today. He did so, in front of a monument his mother helped to erect to honor the 1st Rhode Island Infantry regiment, America's first mostly non-white unit. He too, carried both the burden and the honor of stewardship. His brief moved me deeply, as he told the story of a unit full of people hoping to prove their allegiance and earn their freedom through sacrifice. Many did, but many did not. It made knowing what came after for many of them especially bitter. After his brief, Mr. Robbins reminded me that The American military wouldn't have integrated units like they were during the Revolutionary War again until the Korean War, 166 years later.

Nearly three quarters of a century later the torch would be passed from Daniel Showalter to his grandson, John Showalter. John enlisted in the Union Army in Pennsylvania during the Civil War. However, something I took note of is when comparing his date of birth to his enlistment date is that he would have only been 16 years old when enlisting. This was still illegal during the Civil War, but some units were known to turn a blind eye to the practice. I'm not sure if his chain of command knew or not. It is now a secret him and I (and you) share. Don't tell anybody.

In the Civil war, the demands of Soldiers and NCOs had grown far beyond what the Continental Army had faced. The lessons of Valley Forge laid the foundation, but the scale and complexity of the Civil War would transform the Corps even further. The Union had hundreds of thousands of Soldiers, at one point it is believed they neared one million Troops. NCOs became non-negotiable in these massive formations, and it became paramount that NCOs learn and teach battle drills in order to fight in large scale combat effectively. It was also during this time that every NCO became somewhat of a logistician. After every engagement it was the responsibility of the NCO to check on his men's health, ammo, water, and rations. The earliest form of what we now call the SITREP. Effective first aid became a common point of training within regiments as well. However, a formalized document wouldn't be published until nearly 10 years after the Civil War, leaving each unit to independently scramble to come up with their own techniques. I am unsure of what kind of medical practices were being employed in John's unit, but since it coincides with the times of "you have ghosts in your blood, take this cocaine" my hopes aren't high. Then again, John did survive the Civil War, so maybe it has its merits. After the Civil War he would, in his own lifetime, witness a technological leap that I don't believe has been replicated since. John's war was fought by men on horseback firing rifled muskets, but his son, Frank Showalter, only 49 years later, would be fighting in the trenches of World War I where tanks, planes, long range artillery, and fully automatic machine guns ruled the battlefield.

As a Sergeant during the First World War, Frank found himself with a few new tasks. NCOs now managed Soldiers with specialties, a precursor to the MOS system we have today. Soldiers were not just rank and file infantrymen, but artillerymen, signalman, medics and engineers. NCOs, particularly senior NCOs, also found themselves with the impossible task of maintaining morale in this epic and gruesome conflict. During the closing six months of the war, Soldiers were constantly rotated on and off the front lines. It was hard to keep soldiers heads on straight, let alone keep morale high. However, first sergeants (1SGs) excelled at building and recording positive unit cultures despite the challenges. There are several units still in the Army today that have their roots in the First World War, and its credited to the efforts of dedicated 1SGs that the legacy of units like the "Big Red One" are enshrined in stone. The lessons learned regarding the late publication of official doctrine in the Civil War were fixed during this conflict as well. Shortly after the very first chemical warfare attack the U.S. Army was quick to publish official procedures. The responsibility fell on NCOs to quickly learn doctrine, and train soldiers on field sanitization, gas mask protocols, and the myriad of other unprecedented threats that now ruled what was beginning to look like the battlefields of today. Unfortunately, Sergeant Frank Showalter would not survive the Great War. He was killed in action during the 100 Days Offensive, alongside 26,000 of his brothers in arms. He was survived by one son, Clyde Showalter, whom he had never met.

My grandfather, Clyde Showalter, never intended to join the Army. He revered his father and the sacrifices he had made to his country, but he also felt the impacts of growing up without him. He did not want to do the same to his family. Despite these good intentions, he was drafted into World War II in 1940, where he would be assigned to the same unit I would serve in 78 years later. 2-325 Glider Infantry Regiment of the 82nd airborne Division. For those of you who don't know, glider units were, as the name implies, units who would deploy men out of small planes inside of big planes. The idea being for these men to be able to carry more equipment than the standard Paratrooper, and be able to gracefully land on the ground with enough ammo and equipment for sustained fights. However in practice, gliders hit the ground with the force of a car crash and the glider Soldiers became functionally Paratroopers with concussions. World War II would see a large broadening of NCO responsibilities, mostly due to the draft.

Recruits were brought in, in the hundreds of thousands. It was during this time that basic training became the realm of the NCO, as the larger force necessitated them be given the autonomy to train soldiers in mass. It was also during World War II that Military Occupational Specialties became official, as it was easier to take an accountant from off the street and make him an accountant for the military. However, that baseline standard of every Soldier needing to be able to be an infantryman was more important than ever, thus the early version of what would become the Warrior Skills Level 1 tasks and battle drills were born. To make certain every Soldier, regardless of specialty, all shared the same baseline skills. At the end of the day, Soldiers needed to be capable of extreme violence. Make no mistake, winning wars is done through great logisticians and coordination across various support roles, but at the end of the day, somebody needs to be able to shoot somebody to make all the work matter.

Despite his earlier reservations, he followed in the same footsteps that ultimately killed his father. Clyde would choose to remain in the Army after World War II. Serving as a staff sergeant during the Korean War and a first sergeant during the early years of what would become the Vietnam conflict. 1SG Clyde Showalter would retire from the 82nd airborne division in 1961. I'd be remiss if I didn't mention that just a few years later in 1964, the Drill Sergeant became official, hugely boosting the culture of the NCO Corps in the public perception. However, the tail end of the Vietnam conflict came with some trouble for the NCO Corps. The swap to the all-volunteer force was attributed as a leading factor for this, which confused me greatly. I thought it'd be the opposite, given that the Soldiers fighting had at least wanted to be there. However, due to several factors, the force was in a slump.

1. The Vietnam War was largely unpopular
2. Experienced soldiers left in droves during and after the Vietnam War
3. The "Go to War or go to jail" policy kept a lot of service members in that probably shouldn't have been.

It was due to these factors that the NCO Corps attempted to light a fire in the hearts of NCOs through encouraging intrinsic motivation to serve ones country. They did this through setting a core set of ideals NCOs should live by. It would be to the dismay of thousands of board ready E-4s (specialists) for decades that Sgt. 1st Class (SFC) Earle Brigham would pick up a pen and write the NCO creed in 1973, describing it as "a yardstick by which to measure ourselves against." As we head into the future, we see this trend of the Army instilling its leaders with core principals and ideals to live by continue, with another push coming with the publication of the seven Army Values after the Gulf War.

Clyde Showalter, as I said before, was fortunate enough to retire from the Army. It did not come easily for him though. His tale is of a struggle that is seen over and over again with Soldiers today. A failure to fully transition from Soldier to Citizen. According to my father, Clyde was a much calloused man after the wars. He was not kind, he did not show affection to his sons, and he buried himself in his work, staying away from home weeks at a time. He was abusive, he was distant, and he struggled with undiagnosed PTSD, refusing to admit that he needed help of any kind. This was only made worse when one of his sons, my uncle, would die young in the Vietnam War. Clyde Showalter passed away in 1990 of natural causes. He lived a long and storied life, and was undoubtedly a hero in many regards. My father speaks of him with both reverence, and disdain all at once. He resents his father to an extent, but also acknowledges that he was too young at the time to see the full extent of Clyde's struggles. My Father was only 14 years old when his father passed, thus continuing the cycle of growing up without. My father, in the hopes of both breaking this cycle and not growing up to be the man his father was, chose to not enlist. He took the act of rebellion so far, I will admit my Dad is a bit of a hippie, but we love him for it anyway. My father took great care to not expose me to the Military lifestyle he had grown up in. Unfortunately for him his efforts were in vein, as Michael Bay would release Transformers One in 2007 that would ignite the spark in me. (I am not just referring to Meghan Fox's character in the movie, but the cool military guys fighting giant robots). To the dismay of my father, I enlisted as a junior in High school in the Delayed Entry Program as a 13F, Forward Observer.

Which leads us to where we are today in this post 9/11 world. NCOs faced new challenges in Iraq and Afghanistan. The Infantrymen could no longer just be a door kicker, he needed to be a diplomat, able to effectively communicate across cultural boundaries in order to win hearts and minds during key leader engagements. NCOs need to display strong moral character, as any mistake could and would reflect poorly not just on himself, but his entire organization (read "Blackhearts" by Jim Frederick's to see just how destructive a small group of Soldiers can be on the entirety of the US Military). Any lack of sound judgement would destroy partner relations in such austere and morally dubious environments. Now, NCOs need to be more than just trainers, coaches, mentors, leaders, door kickers, and diplomats. They also need to continuously help their units innovate by leveraging emerging technologies, or else risk letting their units slide down the power curve. We see it now with the explosion of AI in 2023 leading to NCOs hard charging integration efforts at the tactical level.

From the early days of Valley Forge to the Cyber Domain we fight in now, the responsibility of the NCO Corps has only been made greater. The bank of NCO credibility is one you can add to, but that you may never withdraw from. Especially for pleasure, profit, or personal safety. That account balance has been earned through blood, sweat, and spent shell casings. My forefather Daniel served in Valley Forge almost 250 years ago. However, this is not just my history, it is yours. Whether your family has been serving since the beginning, or you are a first generation immigrant to the United States. Today, you stand here, wearing the same stripes, and carrying the same responsibilities as those who came before us. The burden of responsibility for the Army as an organization is a heavy one, and it is our turn to carry it. I hope you also leave behind a legacy your 6x great grandkid will write about. The tools have changed, the battlefields have changed, but the Backbone of the Army remains the same. Thank you for your service.

Reference:

[1]Valley Forge: Steuben, 1778. /Nbaron Friedrich Von Steuben Drilling American Troops At Valley Forge, 1778. After A Mural Painting, C1910, By Edwin Austin Abbey.

The Buy-in

By Sgt. Evangelin A. Samuel, Charlie Company, 781st MI Battalion (Cyber)

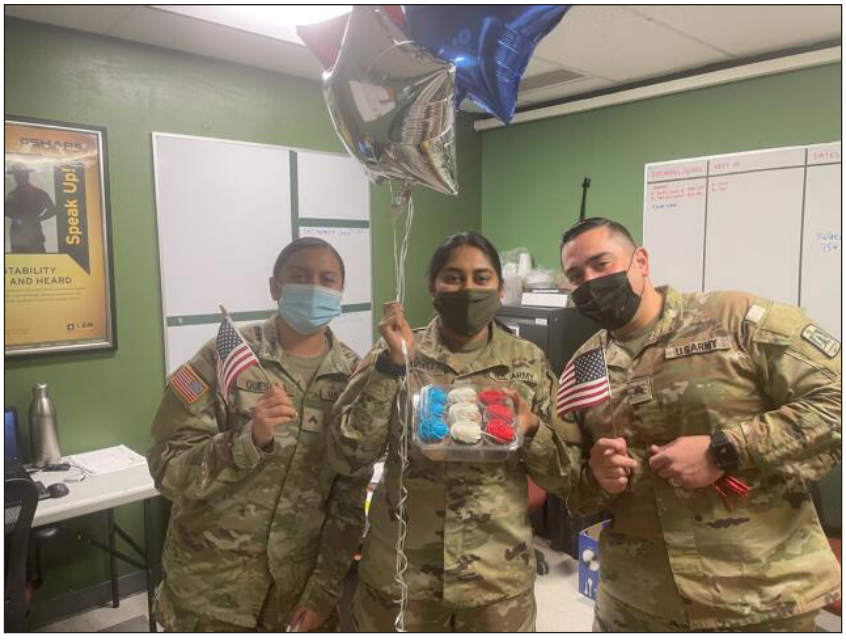
"WHY DID YOU JOIN THE MILITARY?" was one of the first things I was asked when I enlisted and I'm sure you have been asked that at some point in your military career. During Basic training, this question is often revisited to remind Soldiers of their purpose and motivation. When training gets tough and doubts begin to set in, remembering why you joined helps refocus your mindset and gives you strength to push through the challenges. It serves as a personal anchor – a reminder of the goals and reasons that led you to sign that first contract. Reflecting on your "why" builds resilience, reenforces commitment to the mission, and fuels the courage to keep going, no matter how difficult the task becomes.

There are many versions of "why" that I have heard over the years. For some, it is the opportunity to earn money, seek job stability, or receive college benefits like the GI bill. For others, it is out of a deep sense of patriotism, a desire to continue a family legacy of service. Some seek structure and discipline to turn their lives around, while others see the military as a way to travel the world, learn valuable skills, or find purpose and direction. A few join to escape difficult circumstances or avoid negative paths-seeing the military as a second chance to find a better future.

- I ask you today-what makes you stay in?
- Is it completing the goals you set for yourself when you join?
- Is it finishing those last few semesters towards your college degree?
- Is it paying off that car or house?
- Or maybe, it is the thought of retiring proudly, just like your family members before you.
- For some, it's maybe being grateful that the military gave them a second chance and truly turned their life around.

Whatever your reason, never lose sight of it. Your "why" doesn't just get you through Basic Training – it guides you through your career. When things get tough, remember why you started and who you are doing it for.

I love hearing everyone's "why". Hearing what drives others gives me motivation too. I know you are probably wondering what my "why" is, right? For me it was about family, I wanted to take care of my first-generation immigrant family. If I am being honest, my reason was a little short-sighted at first. I joined to find stability, make ends meet and to help at home. Over time it has grown into something much bigger. Now, it is about creating a legacy-about being the first person in my family to ever serve. I feel a sense of pride every time I wear this uniform, and I will keep wearing it as long as they let me. And hopefully my dedication encourages the next generation of my family; and people in my life to also join (or stay in) and continue a legacy that I created when I signed that piece of paper. ■



11th Cyber Battalion Change of Responsibility

By Spc. Teanna Dooley, 11th Cyber Battalion

FORT EISENHOWER, Ga. – Soldiers, Civilians, friends, and Family bade farewell to Command Sgt. Maj. (CSM) Keyne A. Smith, the outgoing command sergeant major of the 11th Cyber Battalion, Leviathans, and welcomed CSM David Herrera Jr., their new senior enlisted leader and 'keeper of the colors', in a ceremony hosted by Lt. Col. (LTC) Charles E. Suslowicz, commander of the 11th Cyber Bn., in Darling Hall, October 03.

LTC Suslowicz told the gathering that the Change of Responsibility ceremony was an important day in the history of the 11th Cyber Bn. as it commemorated the extraordinary service of CSM Smith, "who has guided this battalion with an uncompromising commitment to our Soldiers," and welcomed a new senior enlisted leader, CSM Herrera, who would now take on that "solemn" responsibility.

"There are leaders who supervise and there are leaders who transform," said Suslowicz, looking directly at Smith. "You are the latter. For the last two years you have stood in the center of this formation as a steward of our standards, a relentless advocate for our Soldiers, and the moral compass of this battalion."

The battalion commander then listed the significant changes that had occurred during her tenure including: participating in multiple "successful" Combat Training Center rotations; implementing a sustainable readiness and providing the teams consistency and clear expectations for the months ahead; and the transition of the Remote Cyber Team and Single-Source SIGINT (Signals Intelligence) Team from concept to supporting real-world operations on a daily basis.

"A far cry from concerns, not that long ago, that Soldiers in 11th Cyber Bn. would not be able to 'be on mission'," said Suslowicz.

"Beyond this transformation, your legacy is written in the men and women of the 11th – toughened by your standards, guided by your counsel, and inspired by your example," added Suslowicz. "I know many of our junior NCOs recall a time when you dropped what you were doing to make yourself available as a mentor, personally intervened to help a Soldier in need, or demanded more because you believed they were capable."

After recognizing Smith's Family for their sacrifices and support, which allowed the entire battalion to benefit from their mother's counsel, experience, and insight, Suslowicz thanked CSM Smith, on behalf of the battalion, the Families, and the Soldiers she served day in and day out.

"Distinguished guests, colleagues, family, and friends, thank you for joining today's ceremony. I will not be before you long as I have completed point-to-point engagements to express my gratitude and appreciation, leading up to this moment,' said Smith in her remarks. "However, I must thank God for blessing me and keeping me. Without him, this tour of duty would not have been possible. Thank you to my not-so-little humans, Nyalah and Ty'Son (Smith's children), for pushing me. You make me proud every day and hopefully I have done the same."

In his remarks CSM Herrera thanked his family, past and present leaders, and then ended by addressing the battalion Soldiers.

Herrera remarked that early in his career a leader once told him, "You will not appreciate these moments until they are a memory."

His past leadership, those who had invested their time, energy, and wisdom throughout his career, had shaped the kind of Soldier he strives to be every day: to lead with purpose; to empower leaders; and be accountable and present.

"Lastly, To the Soldiers of the 11th Cyber Battalion, I am humbled by this responsibility and motivated to serve. This is our moment now – so, let's go make some memories. Leviathan 7 signing on the net. ■

Hackathon V – A cyber and computer challenge event for young people

780th Military Intelligence Brigade (Cyber) Public Affairs Office

ODENTON, Md. – Soldiers and Civilians from Fort George G. Meade hosted the last of the three Hackathon events – a program intended to encourage teen interest in STEM (science, technology, engineering, and mathematics), specifically in cybersecurity – at the Odenton Regional Library, Anne Arundel County Public Library.

This is the fifth year the 780th Military Intelligence Brigade (Cyber) hosted Hackathon, and although there was a government furlough, the brigade and garrison Soldiers, all volunteers, flawlessly conducted the events on October 7 and November 4 (the first fall event was held September 22).

The Brigade-sponsored Hackathon centers around a CTF (capture-the-flag) competition, which for the past three seasons has been designed by Chief Warrant Officer 3 Joshua Wellman. The CTF is a 'cyber exercise' where participants search for flags, using a variety of techniques including reverse engineering, decryption, netcat, and ssh keys; and at the four other stations, completing those challenges contributes to their overall CTF score.

"I think, as a dad, it's important for me to teach my kids and other kids useful tools in the real world, and so, whether I'm teaching my kids or somebody else's kids, it's always a good time," said Wellman. "But I think for the brigade, we are part of the community here, so, just like we have our military duties, this is like our duty to the community where we can kind of give back."

The other Hackathon V stations included: a Basic Python table where participants completed python programming challenges; a Publicly Available Information (PAI) table where participants learned to appreciate the perils of posting personal information online and learn techniques for browsing publicly available information; a Logic Games table where participants practiced binary number systems, modulo operations, and Boolean algebra; and there was also a Locksport and ham radio table hosted by the Maryland Mobileers Amateur Radio Club.

"Much appreciation to our partners at Odenton Regional Library, Ms. Sharon Lanasa, Assistant Branch Manager, and Mr. Scott Barter, AACPL. They made coordinating efforts to book library space and equipment seamless. Ms. Lanasa went above and beyond to provide support with advertising the event on the library's website and reaching out to POCs of the neighboring middle and high schools," said event lead, 1st Lt. Akinola Vaughan.

"I would be remiss not to mention the dedication to serve that was displayed by all volunteers, especially the station POCs – CW3 Wellman, 1st Lt. Pranav Balan, Maj. Mark Klink, 1st Lt. Nathan Vowinkel, and Mrs. Ashley Rowe," added Vaughan. "The POCs did a fantastic job with creating/updating the cyber challenges. CW3 Wellman's effort with setting up the Hackathon server and website was pivotal to the success of the event. Mrs. Rowe added a new flavor to the event by introducing Locksport and Maryland Mobileers Youth Amateur Radio Club, which garnered much interest and engagement with the participants."

Annually, the brigade supports more than 15 external engagements, most in support of U.S. Army Recruiting Command's TAIR or Total Army Involvement in Recruiting program; however, other requests for support come through the Fort George G. Meade, Marland; Fort Gordon, Georgia; Joint Base San Antonio, Texas; or Schofield Barracks, Hawaii garrison public affairs offices – installations where the brigade has Soldiers and Civilians assigned; or from our higher headquarters, U.S. Army Intelligence and Security Command and U.S. Army Cyber Command.

The 780th MI Brigade is unique in that we are the Army's only offensive cyberspace operations brigade and we conduct cyberspace operations and capability development to deliver effects in support of Army and Joint requirements.

Praetorians! "Ubique Et Semper In Pugna" Latin for "Everywhere and always fighting" – We don't talk about what we do nor who we are in a cyber 'knife fight' with; however we are *"Everywhere and Always...In the Fight!"*

A huge shout out to Mass Communication Specialist 3rd Class Jackson Wanous who took the November photos and produced the video for his Defense Information School Intermediate Journalism Course project (to see his video and photos visit the brigade's Facebook, *https://www.facebook.com/780MIBDE*; Instagram, *https://www.instagram.com/780mibde_cyber/*, or LinkedIn, *https://www.linkedin.com/company/79685493/pages*). ■

Kids pick locks at the locksport table to test their STEM abilities at the Hackathon at Odenton Regional Library, Odenton, Maryland, Nov. 4, 2025.

The 780th Military Intelligence Brigade (Cyber) hosted the Hackathon at Odenton Regional Library where young participants learned the fundamentals of cybersecurity.

UNLOCKING the FUTUR3 of CYBER DEFEN5E

By: MC3 Jackson Wanous

ODENTON, Md. – It's not every day that kids learn how to hack due to Soldiers. Still, for this Hackathon, it was all about defending the future for the military and civilian world.

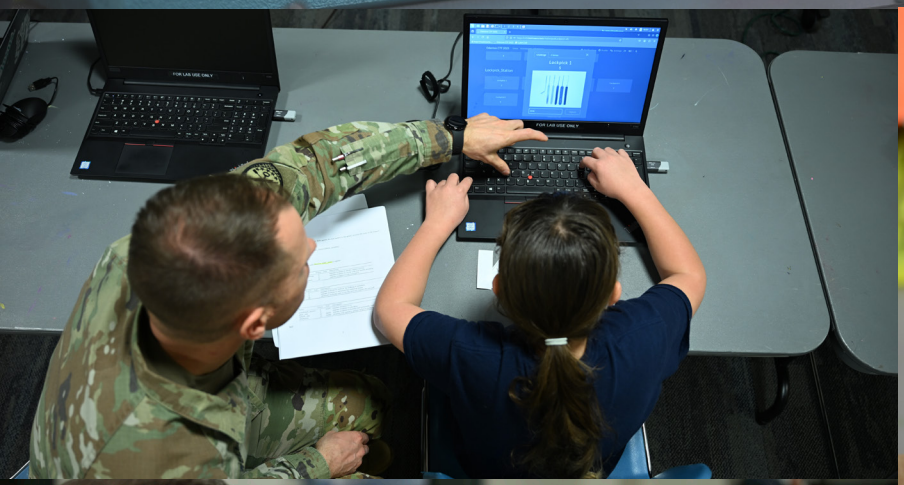
The 780th Military Intelligence Brigade (Cyber) led the Hackathon where volunteers and soldiers taught children of all ages how to use cyber tools both offensively and defensively at the Odenton Regional Library in Odenton, Maryland, on November 4, 2025.

The brigade has held this event three times so far this year. Civilian volunteers and soldiers host the Hackathons to encourage teen interest in science, technology, engineering, and mathematics.

This is the fifth year they have hosted a Hackathon and at the event, participants take part in Capture-the-Flag.

"CTF is traditionally a cyber exercise where you solve various challenges, all typically offensive or defensive related. And in the process of solving the challenge, you're given a flag," Chief Warrant Officer 3 Joshua Wellman, CTF Leader, explained. "You present that flag back to the system for points. The student who ends up with the most points at the end is deemed the winner."

It was Wellmen's third year participating and being with the kids. "I think, as a dad, it's important for me to teach my kids and other kids useful tools in the real world," said Wellman as pride exerted in each breath. "And so, whether I'm teaching my kids or somebody else's kids, it's always a good time."



Cyber Brigade Hires New Government Employees

FORT GEORGE G. MEADE, Md. *- The U.S. Army realizes the importance of the cyber workforce and the 780th Military Intelligence Brigade (Cyber) is doing its part to attract and hire qualified candidates by onboarding ten newly hired Civilian employees at the organization's headquarters, September 22.*

The three cyber capability developers shown here are joining the Operations Support Element's Cyber Solution Development (CSD) detachment in Maryland.

Established as Task Force Praetorian (TF-P) in November 2022, the Task Force was established to consolidate and support the unit's key mission enablers. TF-P was officially approved by the Department of the Army in July 2023 and formally recognized as the U.S. Army Intelligence and Security Command Operations Support Element (OSE) on March 1, 2024. The organization has CSD detachments in Maryland, Georgia, Hawaii, and Texas.

B Company
781st Military Intelligence Battalion (Cyber)
Change of Responsibility Ceremony

FORT GEORGE G. MEADE, Md. *– CPT Daniel Alvarado, commander of B Company (Immortals), 781st Military Intelligence Battalion (Cyber), hosted a change of responsibility ceremony whereby 1SG Angel Rodriguez relinquished his responsibility as the senior enlisted leader to 1SG Nathan Rios, September 25, at the Post Theater.*

"Ubi Ceteri Non Possunt"

Vanguard, When Others Cannot!

Soldiers Awarded for Outstanding Contributions During Training with Cyber Battalion

FORT GORDON, Ga.. *– The 11th Cyber Battalion conducted a validation and communication exercise (VALEX/COMMEX) to enhance mission readiness and validate critical communications systems across its subordinate units from 2 to 5 September.*

The exercise brought together Headquarters and Headquarters Company (HHC), Alpha Company, Bravo Company, and Fort Gordon Advanced Individual Training (AIT) Soldiers for a hands-on, mission-focused communications drill.

According to HS VALEX/COMMEX organizers the AIT servicemembers from Foxtrot Company, 369th Signal Battalion, integrated with the 11 Cyber Battalion and gained valuable experience in configuring and troubleshooting advanced communications equipment. The Soldiers worked with AN/PRC-162 and AN/PRC-152 radios, 1523E ASIP radios, OE-254 antennas, and the Joint Battle Command-Platform (JBC-P).

The following AIT Soldiers were recognized on October 15 for their support during HS VALEX/COMMEX that contributed to the success of the 11th Cyber Battalion's mission: Spc. Antonio Zelaya, Spc. Nicholas Head, Pfc. Steven Lindsay, Pfc. Eugene Figueroa, Pvt. Roland Padock, and Pvt. Kwante Booth

In addition to this recognition, a special commendation was extended to Pfc. Eugene Figueroa for his leadership and initiative throughout the exercise. As a member of Foxtrot Company, Pfc. Figueroa played a key role in leading his peers through complex communications tasks. His ability to troubleshoot systems, guide other AIT Soldiers, and maintain operational focus under pressure which exemplified professionalism and technical competence.

Cyber Battalion Soldiers conduct tear gas training

FORT GORDON, Ga. *– Apex and Bandit Company, 11th Cyber Battalion, conducted a Chemical, Biological, Radiological, and Nuclear (CBRN) confidence exercise as an annual requirement to maintain readiness, October 21.*

Prior to beginning training, the range noncommissioned officer-in charge conducted classroom instruction on their protective equipment and effects of tear (CS) gas. Soldiers then prepared to enter the chamber single file. They were instructed to conduct several exercises followed by removing their protective gear to experience the full effects of CS gas and clearing and resealing their masks. Soldiers then exited the chamber to conduct self-recovery and maintenance protective gear.

Headquarters Company, 11th Cyber Battalion Conducts Day/Night Land Navigation

FORT GORDON, Ga. *– Headquarters Company, Hellhound, 11th Cyber Battalion, conducted Day/Night Land Navigation Training on October 16 and 22 at Training Area 26 (TA26) to enhance Soldier readiness and reinforce foundational field skills.*

The training on Oct. 16 began with Sergeant's Time Training (STT) under daytime conditions. Soldiers were instructed on how to conduct map reading and navigation fundamentals accurately. Once the lesson was completed, Soldiers were required to independently display their knowledge by plotting their points, then navigating through TA26 to locate them.

The second day of training on Oct. 22 introduced night land navigation, which presented a unique set of challenges. With low visibility and no moonlight, Soldiers had to rely on their red lights, map reading, and compass skills to navigate accurately.

Leaders were tasked with guiding their teams through complex routes while maintaining accountability for them. According to the instructors this experience emphasized the importance of clear communication, trust, and effective delegation under pressure.

The Land Navigation training fosters both individual confidence and team cohesion by focusing on hands-on training and practical experience. The event demonstrates the unit's commitment to building operational readiness and ensuring Soldiers and leaders are well-prepared for land navigation and future challenges.

715th MI BN Veterans' Day Headstone Cleaning and Flag Placement

SCHOFIELD BARRACKS, Hawaii *– Soldiers and Family members of Detachment Hawaii (DET-HI), 782nd Military Intelligence Battalion (Cyber), participated in the Veterans' Day Headstone Cleaning and Flag Placement event organized by the 715th MI BN at the Schofield Barracks Cemetery, November 8.*

Soldiers and Family members from DET-HI, 782nd MI BN, along with Soldiers from the 715 MI BN and the Schofield Barracks Cemetery Staff, honored our nation's fallen heroes by cleaning and placing flags on 463 Veterans' headstones. The Soldiers also maintained other headstones – belonging to civilians, POWs, and unknowns – bringing the total to more than 2,600 headstones cleaned by the end of the event.

According to the volunteers the event served to honor our veterans and preserve the dignity of their final resting place through community service and stewardship.

U.S. Army Photos by SGT Susan Nho, DET-HI, 782nd MI BN.

Mele Kalikimaka!

SCHOFIELD BARRACKS, Hawaii *– Detachment Hawaii, 782nd Military Intelligence Battalion entered the U.S. Army Garrison – Hawaii "Holiday Card Lane Contest" with a festive holiday postcard mural featuring the Hyperion logo and a tropical Christmas scene.*

The Holiday Card Lane is a long-standing tradition at Schofield Barracks.

The mural was hand painted by Sarah Smith (SSG Wooden's spouse) and their son Harley. The team is patiently awaiting results of the competition.

Brigades 14th Birthday Celebration

Praetorians,

It is with great pride and gratitude that we celebrate the 14th birthday of the 780th Military Intelligence Brigade (Cyber). This milestone is not just a celebration of our Brigade's history but also a tribute to the men and women who have dedicated themselves to our mission of defending the nation in cyberspace.

Our history is rich with achievements and milestones that have defined us as a premier cyber force. From the re-designation of the 744th MI Battalion to the activation of the 781st MI Battalion and the establishment of Task Force Praetorian, each step in our journey has been marked by innovation, resilience, and a steadfast commitment to excellence.

As we gather to share in the tradition of the Brigade Birthday Cake, let us take a moment to reflect on the importance of our shared history. The cake is more than a symbol of celebration; it represents the unity, strength, and dedication that bind us together as a team.

Thank you for your service, your commitment, and your role in shaping the legacy of the 780th MI Brigade (Cyber). Together, we will continue to honor our history and build a future that reflects the values and mission of the Praetorians.

Very respectfully,
Candy Boparai
COL, CY
Commander, 780th MI BDE (Cyber)

"Everywhere and Always…In the Fight!".

Brigade Army Ten-Miler team

OUR TEAM REPRESENTED THE BRIGADE AT THE 41ST ARMY TEN-MILER WITH DISTINCTION, achieving remarkable results that reflect the dedication, discipline, and teamwork we strive for every day. Our team placed first among all unit teams (non-installation teams) and secured an impressive 12th place out of 33 teams in the Active-Duty Mixed Category. This is an extraordinary accomplishment that highlights the strength and resilience of our Soldiers.

I want to personally recognize the outstanding members of our Army Ten-Miler team:

- CPT Brian Betz (TX) (Team Coordinator and Planning OIC)
- CPT David Kim (GA) (Race Day OIC
- CPT William Mitchell (MD)
- 1LT Charles Boyd (MD)
- LT Christian Fin (MD)
- 2LT Lilian Richards (GA)
- SSG Ariel Dominguez (MD)
- SSG Luke Grays (MD)

Each of these Soldiers demonstrated exceptional commitment and represented our Brigade with pride and professionalism.

It was an honor to witness the team's determination and camaraderie firsthand. Their performance is a testament to the values that make our Brigade strong: teamwork, perseverance, and the relentless pursuit of excellence.

Please join me in congratulating these outstanding Soldiers for their hard work and success. They have inspired us all and brought great pride to the Brigade. CSM Daniel and I are incredibly proud of their achievement, and we look forward to celebrating this success with them and the entire team.

Well done, Army Ten-Miler Team! You have made us all proud.

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

37TH ANNUAL

SATURDAY
MARCH 21, 2026

BATAAN
Memorial Death March

WHITE SANDS MISSILE RANGE

MORE THAN JUST A MARATHON

Looking for a personal challenge, the spirit of competition, or to foster esprit de corps in your unit?

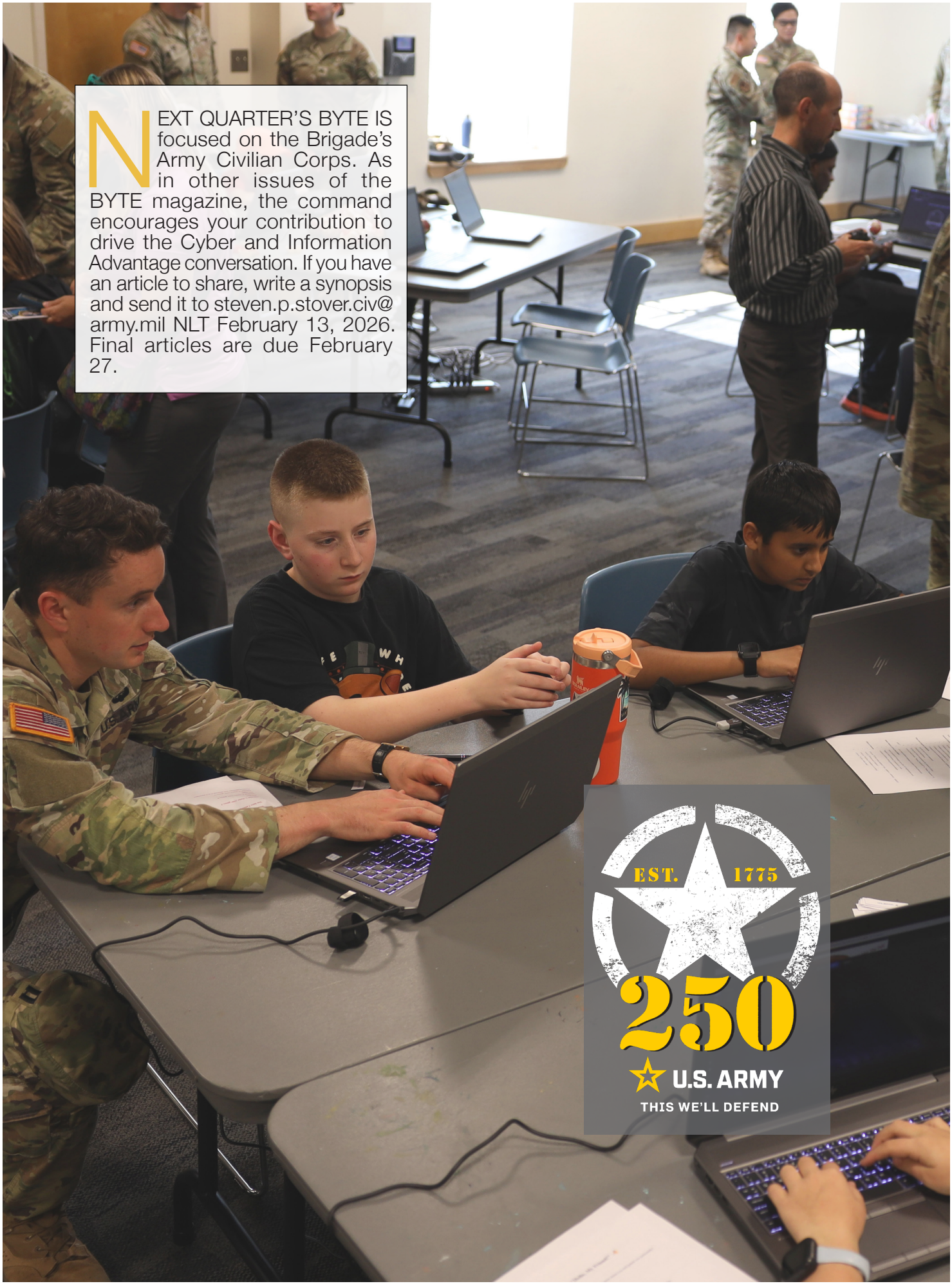
The Brigade is putting together a Bataan Memorial Death March Team to compete in the Military Division Heavy.

Since its inception, the Bataan Memorial Death March's participation has grown from about 100 to about 9,600 marchers. These marchers come from across the United States and several foreign countries. While still primarily a military event, many civilians choose to participate in the challenging march.

It's 26.2 miles of rugged desert terrain, high elevation and weather that can be extreme – with high winds, hot desert sun, or cold temperatures possible. Conquering this course takes a lot of determination, perseverance, inner strength and heart.

Time trials will begin in November and go until January.

Contact your BN S3 for additional information on when and where.



NEXT QUARTER'S BYTE IS focused on the Brigade's Army Civilian Corps. As in other issues of the BYTE magazine, the command encourages your contribution to drive the Cyber and Information Advantage conversation. If you have an article to share, write a synopsis and send it to steven.p.stover.civ@army.mil NLT February 13, 2026. Final articles are due February 27.