780th MILITARY INTELLIGENCE BRIGADE (CYBER)

THE BYTE

Vol. 13, Issue 4

September 2025

LETHALITY: TRAINING AND READINESS

Soldiers / NCOs Responsibilities to Training

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.

780th MILITARY INTELLIGENCE BRIGADE (CYBER)
THE BYTE
Vol. 13, Issue 4
September 2025
250
U.S. ARMY
LETHALITY: TRAINING AND READINESS
Soldiers / NCOs Responsibilities to Training

On the Cover

11th Cyber Battalion:

ARCYBER's Best Squad

WASHINGTON, D.C. – U.S. Army Soldiers assigned to the 11th Cyber Battalion, 780th Military Intelligence Brigade, Army Cyber Command, participate in the Army Fitness Competition in Washington D.C. in honor of the Army's 250th Birthday Parade, June 14, 2025. The U.S. Army's 250th Birthday Celebration will honor the sacrifices, achievements, and enduring spirit of American warriors through a fitness competition, festival, and parade—offering the public an opportunity to engage with Soldiers, Army astronauts, NFL representatives, and Medal of Honor recipients. (U.S. Army photo by Sgt. Macaydan Hawkins)

The brigade's Noncommissioned Officers (NCOs) and enlisted Soldiers were responsible for most of the articles and commentaries in this issue of The BYTE magazine.

Command Sergeant Major Joseph Daniel, Praetorian Seven, the brigade's senior enlisted leader, established the theme for this issue "Lethality – Training and Readiness: NCOs and Soldiers Responsibilities to Training."

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

NCO Training Ownership and Leader Development: The Engine of Lethality

By Command Sgt. Maj. Joseph Daniel, 780th Military Intelligence Brigade (Cyber)

ARMY READINESS is built on disciplined, well-trained, and well-led Soldiers. Across all formations and operational environments, the ability to deliver effects through Cyberspace or mission execution hinges on the proficiency of leaders and the rigor of their training. At the heart of this capability is the Noncommissioned Officer (NCO). More than supervisors, NCOs shape the culture, uphold standards, and drive the training that prepares Soldiers to dominate in warfare. NCOs must fully embrace their role in training and prioritize leader development, they forge units capable of sustained, lethal performance regardless of the mission.

Training Ownership

Training excellence is never accidental, it is the product of intentional planning, disciplined execution, and continuous evaluation. As the Army's frontline trainers, NCOs play a part in every phase of the training process. This ownership begins well before execution. Planning realistic scenarios, securing resources, conducting rehearsals, and ensuring Soldiers are mentally and physically ready are all required to be successful. During training, NCOs supervise execution, correct deficiencies on the spot, and maintain accountability. They safeguard safety, discipline, and integrity, ensuring Soldiers build habits that translate directly to combat effectiveness. Post-training, NCOs lead After Action Reviews (AARs), evaluate performance, and identify gaps. These insights feed into future training cycles, creating a continuous loop of improvement. This deliberate cycle, plan,

execute, assess, refine, is how lethality is built, and NCOs must be the driving force behind it. This is the meaning behind back to the basics.

Leader Development

The Army thrives on leaders who can think critically, act decisively under pressure, and earn the trust of their teams. Leader development is not a checkbox, it is a sustained effort rooted in mentorship, accountability, and experience. NCOs must grow junior Soldiers by providing structured counseling, assigning challenging responsibilities, and delivering feedback that fosters confidence and competence. By empowering junior leaders to plan training, deliver briefings, and make tactical decisions within their scope, cultivates experience necessary for effective leadership. Development also means reinforcing discipline, precision, and adherence to Army Values and the Warrior Ethos. Through consistent mentorship and example, NCOs build leadership depth and ensure continuity in high-tempo environments.

Building Lethality

Lethality extends beyond marksmanship it is forged through disciplined training, cohesive leadership, and unwavering standards. For Cyber units, NCOs build this by ensuring their teams are physically fit, mentally tough, work roll proficient, and confident in their roles. They train Soldiers to master individual and collective tasks, foster cohesion through shared hardship, and perform under pressure. This is how units become capable of defeating any adversary. By enforcing high expectations for timely completion of work roll qualifications and ensuring continued progress in proficiency levels, NCOs prepare Soldiers for the full spectrum of operations. They instill adaptability and initiative, enabling teams to respond to dynamic conditions. In doing so, NCOs do not just build competent Soldiers they build lethal formations capable of delivering decisive results.

Conclusion

Getting a unit to excellence by being good at the basics remains the same for every unit in the Army no matter the mission. Lethality is earned through repetition, discipline, and engaged leadership which all fall under the NCO's charge. Those who take full ownership of training and invest in developing their subordinates are the architects of the Army's most capable and combat-ready units.

11th Cyber Battalion Executes VALEX COMMEX to Validate Tactical Communications

By Cpl. Teanna Dooley and Capt. Julian Tamayo, 11th Cyber Battalion

FORT GORDON, Ga. – The 11th cyber battalion conducted a Validation Exercise (VALEX COMMEX) from September 2 to 5, 2025, to enhance mission readiness and validate critical communications equipment across its organization.

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

Mission Objectives and Execution Over the course of the four-day exercise, Soldiers worked diligently to validate and operationalize key communications systems, including:

- AN/PRC-162 and AN/PRC-152 Radios
- 1523E ASIP Radios
- OE-254 Antennas
- Joint Battle Command-Platform (JBC-P)

Teams loaded mission plans, conducted thorough communications checks, and ensured interoperability across platforms to simulate real-world tactical scenarios. The exercise emphasized precision, speed, and reliability in establishing secure lines of communication under pressure.

Training and Readiness The COMMEX served as a vital opportunity for AIT Soldiers from FOXTROT Company, 369 Battalion to integrate with seasoned operators, gaining firsthand experience in configuring and troubleshooting advanced communications gear. The Soldiers will also participate in upcoming field training exercises as the RETRANS team during daytime operations. This training will provide valuable experience as they prepare to PCS to their permanent duty stations.

Looking Ahead With the successful completion of the VALEX COMMEX, the 11th Cyber Battalion continues to solidify its role as a leading force in tactical cyber operations. The lessons learned and systems validated during this exercise will directly support upcoming missions and ensure the battalion remains agile, connected, and mission-ready. ■

SOLANO
U.S. ARMY

Unleashing Leviathan Drone Dominance

By Sgt. 1st Class William A. Gregory, Sgt.1st Class David A. Jones, Sgt. Joshua R. Hartung, and Spc. Christopher R. Adkins, 11th Cyber Battalion

AS SOLDIERS AND NON-COMMISSIONED OFFICERS (NCOS), our core responsibility is to embody and enforce the principles of lethality through rigorous training and unwavering readiness. This means not just maintaining physical and tactical proficiency but actively embracing emerging technologies that amplify our combat effectiveness. In our Battalion, the Small Unmanned Aircraft System (SUAS) Training Program stands as a prime example of this commitment. It cultivates a combat-ready force primed for rapid deployment, enabling unmanned aerial Electromagnetic Reconnaissance (EMR) and Intelligence, Surveillance, and Reconnaissance (ISR) missions that support global operational demands. By certifying SUAS Operators within our Cyber Teams, we ensure that every team member is equipped to operate these systems with precision, turning potential vulnerabilities into decisive advantages on the battlefield.

The SUAS program goes beyond basic certification; it establishes standardized processes for employment and operations while integrating Cyber Electromagnetic Activities (CEMA) payloads to extend tactical range capabilities. Aligned with objective performance standards, this training directly influences equipment procurement and deployment strategies, fostering an environment where innovation meets practicality. For NCOs, this translates to hands-on leadership in drills and simulations, where we guide Soldiers through real-world scenarios that demand adaptability and technical mastery. It's our duty to instill discipline in these sessions, ensuring that operators can seamlessly fuse drone intelligence with ground operations, thereby enhancing unit cohesion and mission success.

Recent directives from the highest levels underscore the urgency of this focus. The Secretary of Defense's memo, "Unleashing U.S. Military Drone Dominance," issued on July 10, 2025, calls for a sweeping expansion of small, low-cost drone usage to counter adversaries' rapid advancements. By rescinding bureaucratic hurdles and empowering warfighters with direct procurement authority, the memo aligns perfectly with our SUAS initiatives, accelerating the integration of American-made drones into training regimens. This policy shift bolsters our program's emphasis on "train as we fight," incorporating force-on-force "drone wars" simulations by 2026, which will sharpen our lethality against evolving threats seen in conflicts like Ukraine.

Ultimately, by prioritizing SUAS training and leveraging the SecDef's vision, we provide Ground Force Commanders with flexible, scalable sensing options that elevate battlefield awareness and informed decision-making. As Soldiers and NCOs, our responsibility extends to mentoring the next generation in these capabilities, ensuring our Brigade remains at the forefront of modern warfare. This dedication to training and readiness isn't just about survival—it's about dominating the fight, turning every operation into a testament to our lethal edge.

Leviathan
Global Reach, Global Impact ■

From Fundamentals to Advanced: My Path Through the Analyst Pipeline

By Staff Sgt. Eli Marvin, exploitation analyst, 11th Cyber Battalion

WHEN I FIRST STEPPED INTO the Digital Network Exploitation Analyst (DNEA) pipeline, I did not fully realize how much it would shape not only the way I think, but also the way I plan and approach problems. The process is demanding, but it is also one of the most rewarding professional experiences I have had in the Army. By the time I finished, I understood what it meant to take broad, sometimes incomplete data and turn it into something leaders could use to create advantage and meet objectives.

The DNEA Pipeline

The DNEA track is about building fundamentals. On average, it takes about a year to move through, but that isn't a hard timeline – it depends on course availability and how quickly you work through your Job Qualification Record (JQR). The JQR is a large checklist of knowledge, skills, and abilities (KSAs) trainers sign off as you demonstrate proficiency.

Two series of courses stood out as foundational pillars:

- **Technology Fundamentals for Analysis (NETA)** – establishes the technical baseline needed to navigate diverse digital environments.
- **Basic Analytic Reporting (RPTG)** – reinforces the ability to structure information into intel-oriented products.

DNEAs are often the first link in the intelligence chain, and that role demands rigor in both thought and delivery. The pipeline was designed to build exactly that.

Learning from EAs and Warrant Officers

When I moved into an Exploitation Analyst (EA) environment, the biggest lesson came from watching my warrant officers work. They collaborated constantly – looping in developers, engineers, and analysts across the community. Their effectiveness was not about knowing every system; it was about knowing who to reach and how to frame the right question.

EAs write reports too, but they aren't the same as DNEA products. Instead of highly structured formats, EA reports are more like summaries – condensed, fast-moving pieces that translate intelligence into actions or options for decision-makers. Just as important, EAs feed those results back into the intelligence machine, where they influence planning, analysis, and future efforts.

Seeing that up close taught me that lack of experience doesn't disqualify you from contributing. It just means you need to be slow and deliberate until you have built the repetitions. The warrants modeled that: collaboration and clarity over trying to be a one-person encyclopedia.

From Fundamental to Advanced

A basic DNEA has already completed a large portion of the EA pipeline course requirements. That overlap is intentional – it ensures shared foundations before analysts step into a broader scope and a faster tempo.

The Army's updated JQR framework makes the progression explicit: **DNEA is a "Fundamental JQR,"** while **EA and Operator tracks are "Advanced JQRs."** In practice, the fundamentals – structured analysis, critical thinking, and disciplined communication – do not disappear at the advanced level; they become the platform for faster decisions and higher-consequence work.

Training, Readiness, and Support

Pipelines don't run themselves. Serving as a training manager showed me how much coordination it takes to keep Soldiers on track. I sent countless submissions for course seats -sometimes needing corrections – and **780th MI Brigade's S3** was consistently responsive, hashing out details and getting Soldiers into the right training. That consistency is a big reason our **35N-heavy section** (with a smaller number of 17Cs) thrived. Both MOSs feed the DNEA role, but success depended on the partnership between our training shop and theirs.

DNEAs and EAs do not do the same job, but they start from the same place. The shared fundamentals connect analysts across MOS (35N, 17C) and work roles (DNEA, EA). That common analytic language is what keeps the machine running smoothly, even as people shift roles and missions evolve.

The analyst journey – whether DNEA or EA – is not about checking boxes. It is about learning how to feed the intelligence machine, and then how to turn finished intelligence into concrete options. For me, the fundamentals came first, and they continue to guide the way I engage at the advanced level. That is the Army's cyber edge: a workforce built on strong foundations, ready to adapt to mission demands. ■

NCO Responsibilities in Training – Leadership in the Cyber Domain

By Pfc. Max Crisp, 781st Military Intelligence Battalion (Cyber)

Leadership in the Cyber Domain

LEADERSHIP IN THE CYBER DOMAIN presents unique challenges across the chain of command, especially for Non-Commissioned Officers (NCOs). Lethality in this domain demands that NCOs lead with both technical expertise and tactical precision. Beyond standard leadership responsibilities, cyber NCOs are tasked with translating evolving mission requirements into actionable training objectives. This article focuses on how NCOs in the 781st MI Battalion enforce readiness by managing Work Role Qualifications, mentoring junior Soldiers in real-world environments, and maintaining the physical readiness of troops within a largely sedentary work environment.

Work Role Qualification

NCOs ensure troop readiness by facilitating courses such as CNMF-U Analyst101, which helps new Soldiers achieve Joint Qualification Readiness (JQR) status. Analyst101 is a 781st MI Battalion-facilitated course that supports the JQR training pipeline for specific job roles. This course places unqualified Soldiers into back-to-back training sessions directly tied to the JQR process, enabling efficient batch training for small groups. Qualified NCOs facilitate Analyst101, offering mentorship and translating course skills into mission-relevant applications. The course spans multiple sessions over a month, allowing attendees to earn JQR status in their work role. Soldiers unable to attend CNMF-U – which is offered quarterly – work closely with their NCOs to locate and reserve alternative classes, ensuring continuous progression.

Mentorship

Mentorship is critical for junior Soldiers across all job fields, and cyber NCOs play a vital role in this area. They coordinate training within Persistent Training Environments (PTEs) that simulate real mission conditions, allowing junior Soldiers to develop the mental agility and technical skills necessary for success. The PTE emphasizes the Army's principle that Soldiers should "train how they fight." Cyber NCOs are responsible for pushing their teams toward mastery, leading by example in their pursuit of technical excellence and mission readiness.

Physical Readiness

Physical readiness is an essential, though often overlooked, component of cyber force lethality. Cyber roles are predominantly sedentary, requiring Soldiers to spend extended periods at keyboards during mission tasks and training. This makes physical fitness and overall wellness even more critical. NCOs must promote and maintain physical readiness, not only for personal health but also for the strength and resilience of their Soldiers. The 781st MI Battalion addresses this challenge through weekly battalion-wide physical training sessions and daily workouts led by squad leaders. Physical training varies from sports and group runs to weightlifting and ruck marches, encouraging a balanced approach to physical activity and recovery.

NCOs are the backbone of the military leadership structure, tasked with guiding and developing Soldiers at every level. This holds true in the cyber domain, where NCOs manage the JQR process, mentor junior Soldiers, and uphold physical readiness standards. The 781st MI Battalion emphasizes placing NCOs with strong leadership qualities in key positions to foster these standards, ensuring mission-ready teams capable of operating effectively in contested digital environments. ■

Readiness by Design: A Soldier's Perspective on Cyber Lethality in the 781st MI Battalion

By 2nd Lt. Mehr Tamboly, 781st Military Intelligence Battalion (Cyber)

IN THE 781ST MILITARY INTELLIGENCE BATTALION (CYBER), every Soldier is a critical node in the Army's cyber lethality. Success in cyberspace operations hinges not only on advanced technology but also on the readiness, technical proficiency, and mindset of the individual behind the keyboard. From the moment a Soldier arrives, they are expected to own their development and contribute directly to national-level cyberspace operations.

Owning Technical Development

Readiness begins with the Job Qualification Record (JQR) a structured, mission-aligned process that outlines the technical skills and operational knowledge required for a Soldier's specific cyber work role. More than a checklist, the JQR is a developmental tool that helps Soldiers and leaders identify skill gaps, tailor individual training plans, and measure progress toward mission readiness.

Every Soldier is expected to take personal responsibility for progressing through their JQR. Whether training as an Exploitation Analyst (EA), Digital Network Exploitation Analyst (DNEA), or Interactive On-Net Operator (ION), Soldiers know that qualification is not simply a requirement, it is a baseline indicator of their ability to contribute to the mission.

Mission-Aligned Training & Hands-On Keyboard Time

Training in the 781st MI Battalion is deliberately aligned with real-world mission demands. Soldiers are immersed in Persistent Cyber Training Environments (PCTEs) that replicate the complexity, uncertainty, and tempo of actual cyber operations. These environments are designed to test technical knowledge, sharpen problem-solving, and foster adaptability under pressure.

Hands on keyboard time is not occasional it is integral. Soldiers practice live scenarios, execute simulated missions, and conduct tool-based replications of known threat behaviors. This continuous, immersive training ensures that when real operations occur, Soldiers are not experiencing something new, they are executing what they have already practiced.

Work Role Qualification: Readiness Beyond Certification

Following the JQR, Soldiers work toward Work Role Qualification, a higher standard that validates their ability to operate effectively within their assigned role. Work Role Qualification is a culmination of mission support, peer evaluation, tool mastery, and tactical decision-making. Achieving this qualification confirms that a Soldier is not only trained, but combat-effective in a full-spectrum Cyber mission set.

JCC2R: Cyber Readiness Validated Under Fire

A distinguishing feature of the 781st's readiness model is participation in the Joint Cyber Common Core Readiness Review (JCC2R). This comprehensive validation event tests Soldiers against mission-essential tasks in contested and dynamic cyberspace scenarios. The JCC2R is designed to reflect real-world operational challenges, ranging from hostile network environments to rapid threat shifts, and assesses a Soldier's ability to maneuver, analyze, and act with precision and speed.

As one participant explained: "JCC2R isn't just a test, it's a reflection of how ready you really are when it counts."

Badging & Integration: Building Mission-Effective Teams

Readiness does not end with individual training. The badging and integration process is a critical bridge from qualification to mission contribution. Once Soldiers complete their JQR and achieve work role certification, they undergo a structured integration process where they receive mission-specific access, tool orientation, and cross-functional onboarding.

This process ensures that Soldiers are embedded into teams with clear expectations and immediate impact. It reduces ramp-up time and helps foster operational continuity, team trust, and technical agility across all mission elements.

Operational Engagement and Feedback Loops

Unlike traditional units where training and operations are distinct phases, in the 781st MI Battalion they are tightly interwoven. Soldiers are actively engaged in ongoing operations, and frequently provide feedback to refine tools, adjust TTPs, and iterate training pipelines. This mission-development loop ensures that training evolves as fast as the operational landscape does.

As SPC [REDACTED], a Cyber Operations Specialist, put it: "You're not waiting for training to come to you. You're expected to seek it, master it, and apply it. You don't just train to be ready, you train to win."

Conclusion: Cyber Lethality Starts with the Soldier

In the 781st MI Battalion, readiness is not accidental, it is deliberate, persistent, and mission focused. Through rigorous training, hands on cyber experience, validated qualification processes, and immediate operational integration, every Soldier becomes a critical enabler of Army cyber lethality.

Each Soldier's readiness is not just a personal achievement; it is a strategic asset. Whether conducting defensive cyber operations or enabling offensive effects in contested environments, the readiness of the individual directly impacts national security outcomes. ■

Cicero's De Officiis – Lessons for the Modern Officer

By Capt. John Bernard McClorey, 403 CMT Operations Officer, Detachment Texas, 782d MI BN (CY)

MARCUS TULLIUS CICERO was a prominent roman statesman known for his political acumen and art of persuasion. He wrote perhaps his most famous treatise, De Officiis, as a guide for good conduct in public office. The Latin "de officiis" translates to English as "on offices," "on obligations," or "on duties." Officers in our United States Army, commissioned or non-commissioned, may find Cicero's stoic insights useful in contemplating the duties of their profession, reinforcing good conduct, and correcting bad conduct. Cicero wrote De Officiis during the tumult following the assassination of Julius Caesar, exploring the apparent conflict between moral behavior and expediency. He argues, however, that moral behavior is unequivocally the most pragmatic course of action. Leadership in Army Cyber operates within an oftentimes hazy chain of command, between administrative and operational control in the upper echelons, and between rank, experience, and certification in the lower echelons. In this dynamic environment, leaders must always default to honorable behavior. Leaders will be tempted to behave disingenuously to accomplish some objective, but in doing so, risk their own moral standing in the chain of command.

Book 1

Cicero asserts that of all the philosophical topics of contemplation and discussion, obligations seem to have the widest application: "... there is no aspect of life, public or private, civic or domestic, which can be without its obligation, whether in our individual concerns or in relations with our neighbor." (p. 4) Cicero begins his discourse with a definition of obligation, namely as "the highest aim among goods" as well as "the moral guidance which can shape our daily lives in all their aspects." (p. 5) Cicero acknowledges that obligations fall on scale, some more absolute than others. He classifies absolute obligation as 'the right,' or katorthama in Greek, and meson for intermediate, ordinary obligation. (p. 5) Cicero cites the Stoic philosopher, Panaetius of Rhodes, who described how we consider courses of action. First, we discern whether the action is right; second, whether the action is beneficial; and then the third, which gives pause, when we discern whether what is right is truly useful. Ostensible conflict between the honorable and the useful plagues action and perpetuates indecision. (p. 6) In laying the groundwork for this treatise on obligations, Cicero necessarily defines the nature of Man as being reasonable, and that this characteristic differentiates humankind from other earthly creatures. We visualize consequences and detect the causes of things, seeing and charting the course of our lives. A "surpassing love" of family drives Man to protect and perform tasks. But finally, and most characteristic of humankind is the search for Truth and appreciation of beauty: "Associated with this eagerness for the vision of the truth is a kind of aspiration for leadership, so that the mind well fashioned by nature is willing to obey only a moral guide or teacher or commander who issues just and lawful orders for our benefit." (p. 7)

Cicero instructs that honorableness derives from four sources: intelligence of what is true, justice (rendering to someone that which he deserves), possession of a "lofty and unconquered spirit," and unflappable temperance reflective of moderation and self-control. He explains, "...the more clearly a person sees the essential truth of a situation, and the keener and swifter is his ability to grasp and explain its logic, the more prudent and wise he is commonly and justifiably regarded." (p. 8) Cicero describes justice as "the brightest adornment of virtue," and its "closest companion" as beneficence, or kindness and generosity. The delivery of justice must always be accompanied by genuine care for the person receiving what they are due. Justice without beneficence is hardly justice. Later, Cicero asserts "nothing is more praiseworthy or worthy of a noble and exemplary man than to be conciliatory and forgiving… All punishment and rebuke must be free of insult." (p.31)

Cicero proceeds to classify benevolence, munificence, and generosity. He advises that benevolence should not go beyond means and is properly "apportioned to each recipient according to his worth." (p. 17) Ordered benevolence in this sense is just, or properly rendered in proportion, to what is deserved. Benevolence in excess of what is deserved is fraudulent, disingenuous, and indeed, unjust. Cicero identifies two types of injustice, one achieved by force, but the other through deceit. False benevolence falls into the latter category: "deceit is the more odious; of all kinds of injustice none is more pernicious than that shown by people who pose as good men…" (p. 17) Normalizing this philosophy to the Army and Army Cyber, leaders must be especially careful to discern matters of justice in praise, reward, and discipline to members of their formations. Excess praise and lack of due discipline disservice Soldiers and adversely affect the mission. At the same time, leaders must recognize and reward Soldiers for jobs excellently done.

Cicero addresses the subject of friendship, which he describes as the "strongest bond of fellowship." Citing Pythagoras, he observes that "when two people have the same ideals and aspirations, they take the same pleasure in each other as in themselves… that though more than one we become one." (p. 21) In this classical sense of friendship, leaders must endeavor to unite themselves with their formation. In a diverse Army with Soldiers from many different viewpoints, backgrounds, and value systems, unification may prove difficult. What unites, however, is belief in and motivation to accomplish the mission. The charge of a leader, easier said than done, is to create a culture of classical friendship amidst a wide variety of these obstacles. Accomplishing such a culture requires contemplation, intentionality, and tactic. Leaders do not establish a culture of friendship merely by "winging it."

Cicero describes the spirit of great and courageous individuals, which is defined by two primary features. The first feature is a "disregard for external circumstances," only regarding oneself with the honorable. This ironclad caste of character is the root cause for greatness. (p. 24) Later in the treatise, however, Cicero seems to make a contrary point: "Disregard for what others feel about you is a mark not merely of conceit but also of lack of integrity." (p. 34) So which is it? Cicero's paradox reflects an Aristotelian concept of 'the mean,' or a ponderance of the middle between extremes. Often, right action is discerned in a grey area – a great leader should disregard anything that is not totally honorable, but at the same time, have considerable mind for the perception of others. Once you have attained an unflappable disposition, the second feature of a magnanimous spirit is engagement in difficult and meaningful work. (p. 24) Army leaders should strive to achieve the decorum (meaning 'the fitting') of a magnanimous soul as Cicero describes. (p. 33) Magnanimity requires restraint, calm, temperance, and prudence, when it would be otherwise tempting to engage in panic or anger or any other host of unhinged emotions. Tempering oneself and then having the gumption to engage hardship head-on is the mark of greatness. Cicero compares two poetic heroes, Ulysses and Ajax. Ulysses endured scorn from all, but dealt pleasantly and courteously at all times until he achieved his goal. Ajax on the other hand, "with that fabled temper of his would have preferred to face death a thousand times rather than endure such treatment." (p. 39) Cicero advises each person to regulate according to his own characteristics, "for a person's most distinctive characteristics are what suit him best." (p. 39) A great leader understands his own extremes, whether a Ulysses or an Ajax, and then must reign himself in. Along these lines, Cicero also makes an elegant argument in favor of PT! "[The] integrity which we demand from a lofty and high-souled spirit is the fruit of strength of mind rather than of body, yet we must train and discipline the body to ensure that it can obey counsel and reason in the performance of business and the endurance of hard work." (p. 28) Even if our profession does not necessarily entail heroic physical fitness, maximal leadership requires a healthy and trained physical presence. What's more, "a dignified appearance is to be maintained by the healthy complexion which is the outcome of physical fitness." Cicero even comments on rules for movement, alluding again to Aristotle's golden mean: "We must be careful… not to saunter along too mincingly, looking like the tray-bearers in pubic processions, nor again to hurry along at breakneck speed so that we puff and blow, go red in the face, wear agonized expressions – all indicating clearly that we lack fixed purpose." (p. 44)

Finally, Cicero discusses the importance of young people to seek guidance and for elderly people to provide sage advice. He describes the importance of mentorship: "a young man's obligation… is to respect his elders, and to choose from among them the best and most highly proved, on whose advice and authority to rely, for the ignorance of early manhood should be stabilized and governed by the wisdom of the old." (p. 42) Young Army professionals should seek guidance from exceptional seniors, and senior officers must offer sage advice to the greatest possible extent to the youth.

Book 2

Cicero continues his study on obligations with an examination of expediency, or the level of usefulness of a thing. He introduces a chain syllogism: "what is just is also useful, and again that what is honourable is also just. The conclusion from this is that whatever is honourable is also useful." He then delivers some strong words for those who do not align with this logic: "Those who fail to see this are people who often venerate tricksters, and mistake perversity for wisdom." These people must come to realize that they will achieve their ends not by evildoing or deceit, but by justice and honor. (p. 58) He takes the position opposite to Machiavelli, the notorious Italian Renaissance philosopher, who posited it better to be feared than loved. Cicero cites the Roman poet, Quintus Ennius: "Him who they fear, they hate; and him whom all men hate they would see dead." (p. 61) In this manner, Cicero calls for fear to "be banished, and affection be preserved, for in this way we shall most easily fulfil our aspirations in both private and public life." (p. 62) To garner the affection of followers, leaders must display goodwill, rendering services and having a true desire to serve: "What strongly rouses the affection of the masses is the actual report and reputation which a person has for generosity, kindness, justice, good faith, and all the virtues associated with civilized and affable manners." (p. 65) Admiration is attained by leaders who "excel in merit, distance themselves from disgrace, and withstand vices which others find hard to resist." (p. 66) Likewise, followers trust leaders who are both just and prudent. Full trust cannot be established without these virtues in tandem. Followers must be confident in the decision-making capacity of the leader, as well as the leader's resistance to deceitful behavior.

Book 3

Cicero concludes his study on obligations in a third and final book. He discusses the topic of secrecy. If one were able to hide his actions from the gods themselves, would it still be advantageous to behave honorably? To address this conundrum, Cicero invokes the story of Lydian King Gyges who, according to Platonic legend, happened upon the corpse of a man wearing a magnificent gold ring. Gyges took the ring for his own, and discovered that when he turned the bezel, he would become invisible. J.R.R. Tolkien, the author of The Lord of the Rings, took inspiration from this story. Gyges used the ring to engage in all kinds of undetected, illicit behavior, eventually achieving the Lydian throne. Cicero settles on moral order, explaining that it is unequivocally disadvantageous to commit evil. Even if there is material gain to be had by acting deceitfully, behaving in discordance with virtue compromises the vitality of the individual's very soul and the security of others in Society.

"If justice must be set aside, to win the throne, let it be set aside; fear God in other things." (p. 112)

References:

[1]HCicero, Marcus Tullius. On Obligations: De Officiis. Translated by P.G. Walsh. Oxford: Oxford University Press, 2008. ■

Sustaining Cyber Superiority Through Lethality and Force Readiness

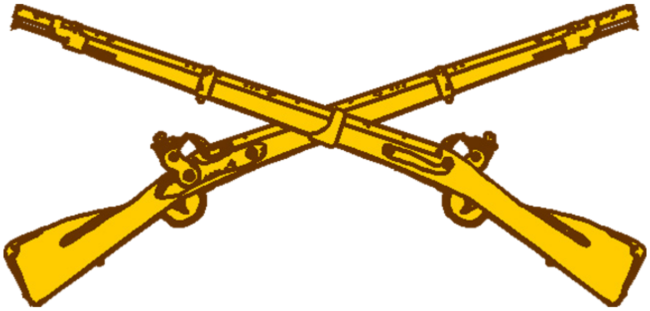
By 1st Sgt. Nevada C. Henricksen, Master Sgt. Cory D. Lindsay, and Sgt. 1st Class Wyatt C. Wolfe, Detachment Hawaii, 782d MI BN (CY)

THE UNITED STATES ARMY AND THE 780TH MILITARY INTELLIGENCE BRIGADE (CYBER) possess a unique capacity to generate, deploy, and sustain cyberspace effects unmatched by our adversaries, delivering a decisive operational advantage to commanders. This is achieved by integrating lethality, training, and readiness.

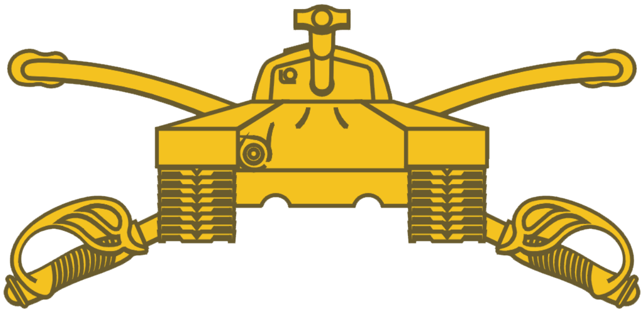
Although the Brigade does not directly align with Armored or Infantry Brigade Combat Teams, our operational equivalency remains similar. Army units build from the team level to a Brigade culminating exercise. Cyber follows this same progression but stops at the company level due to operational structure. Traditional Army units conduct Field Training Exercises (FTXs), live-fire ranges, and squad drills. Cyber builds lethality through Mission Readiness Exercises (MRX), Mission Rehearsal Exercises (MRE), and Operational Readiness Assessments (ORA), in addition to meeting Job Qualification Requirements (JQR).

Cyber leaders have often sought to differentiate themselves from combat arms counterparts by changing language, mindset, and philosophy. In reality, our approach parallels theirs. While we do not execute infantry-specific battle drills such as reacting to direct fire, conducting platoon assaults, or breaking contact, we do perform our own mission-critical skills and drills – captured as work role proficiency levels in systems of record like Joint Cyber Command and Control (JCC2). JCC2 provides leaders with an immediate snapshot of readiness, enabling them to ensure we remain the most trained, lethal, and ready force available.

To increase combat power and lethality for the Joint Force Commander, we should close the gap with combat arms by conducting an annual "sustainment" digital gunnery. Less demanding than an ORA, these internal (Company/Detachment) graded events could measure our effectiveness against simulated adversary targets, like how an M1A2 SEP v3 platoon evaluates performance on a gunnery range. Grading criteria could include identifying target personas and network node functions. These sustainment gunneries lasting one to five days would expand our readiness and lethality for the future. ■



Infantry Branch



Armor Branch

Cyber Branch

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.

The Uniqueness of Lethality, Training, and Readiness in the U.S. Army's Cyber Workforce

IN AN ERA WHERE WARFARE EXTENDS beyond physical battlefields into the digital realm, the U.S. Army's cyber workforce stands as a critical pillar of national defense. Led by U.S. Army Cyber Command (ARCYBER), this specialized force operates, defends, attacks, influences, and informs in cyberspace, electromagnetic warfare, and information operations. Unlike traditional combat arms, cyber Soldiers leverage intellect, innovation, and technical mastery to achieve dominance in a domain where actions can disrupt enemy systems without firing a single shot. This article explores the unique aspects of lethality, training, and readiness within the Army's cyber workforce, highlighting how these elements enable the force to adapt to emerging threats and maintain a decisive edge as of August 2025.

The Uniqueness of Lethality: Precision in the Digital Battlespace

Lethality in the cyber domain differs fundamentally from conventional warfare. While traditional lethality involves kinetic force – bullets, bombs, and maneuvers – cyber lethality focuses on non-kinetic effects that can paralyze adversaries' command and control, communications, and critical infrastructure. For the U.S. Army, this means gaining an information advantage in cyberspace while denying it to foes, integrating cyber operations into multidomain environments that span land, air, sea, space, and information. This uniqueness lies in its subtlety and scalability: a well-executed cyber operation can create "windows of opportunity" for warfighters by simulating attacks to expose vulnerabilities, thereby enhancing overall battlefield coordination and strategic decision-making.

A prime example is Exercise African Lion 2025, where U.S. Army Reserve Cyber Protection Brigade personnel conducted the first joint, combined cyber exchange with Tunisian Armed Forces. This multidomain training emphasized offensive cyber operations – often underemphasized compared to defense – alongside incident response and forensics, fostering interoperability across nations and domains. Such exercises underscore the Army's reliance on cyber to support over 50 percent of U.S. cyberspace operations, transforming data into actionable intelligence for commanders.

Moreover, lethality is amplified through data-driven precision. The Department of Defense (DOD) Cyber Workforce Framework (DCWF) categorizes roles across cybersecurity, IT, cyber effects, and more, using analytics to predict threats and optimize force effectiveness. Unlike adversaries who may prioritize quantity, the U.S. Army emphasizes quality – recruiting agile, innovative experts who can outthink opponents in dynamic environments. This intellectual lethality ensures cyber forces contribute directly to unified land operations, denying adversaries' advantages and enhancing the Army's overall combat power.

Training: Forging Experts through Specialized and Adaptive Programs

Training for the Army's cyber workforce is uniquely tailored to blend technical proficiency with a warrior ethos, preparing Soldiers for a battlespace where threats evolve rapidly. The U.S. Army Cyber Center of Excellence (CCoE) at Fort Gordon, Georgia serves as the hub, transforming traditional signal training into a cyber-focused "university model" that develops adaptive leaders. Programs emphasize certifications, simulations, and continuous learning, ensuring personnel can secure networks, mitigate risks, and execute offensive operations.

Key training initiatives include:

- DOD 8140 Cyberspace Workforce Qualification Program: This agile framework offers over 300 qualification options, validating skills through training, education, and certifications to maintain lethality against sophisticated threats. It shifts training "to the left," reducing on-the-job learning and accelerating operational integration.
- Security+ Certification Course: A one-week program at CCoE that equips Information Assurance Workforce members with skills in threat analysis, secure network administration, cryptography, and the CIA Triad (Confidentiality, Integrity, Availability). This meets IAT Level 2 requirements for DOD networks, directly boosting readiness by enabling secure operations and risk mitigation.
- Persistent Cyber Training Environment (PCTE): A platform for individual sustainment training, team certification, and mission rehearsals, simulating real-world cyber scenarios to hone offensive and defensive skills.

Uniqueness stems from the integration of cyber into broader leader development, such as Basic Officer Leader Course and Captain's Career Course, where trainees learn to incorporate cyberspace into multidomain planning. Internships and fellowships provide hands-on experience, while partnerships with NSA and DISA ensure cutting-edge curricula. This approach fosters a data-literate force, with AI-enabled education pipelines progressing from basic to proficiency over 48+ months, emphasizing innovation over rote learning.

Readiness: Building a Resilient and Agile Force

Readiness in the cyber workforce is measured not just by numbers but by qualification, adaptability, and holistic well-being, ensuring the force can deploy, fight, and win in contested environments. ARCYBER employs data analytics via platforms like Advana to track over 50 KPIs, including vacancy rates, training completion, and proficiency levels across 73 DCWF roles. The first Cyber Health and Readiness Report, launched in February 2025, assesses foundational readiness, with expansions planned for 2026 to cover 90% of capabilities.

Unique to cyber readiness is the emphasis on cognitive and mental resilience. The Holistic Health and Fitness (H2F) program, adapted for ARCYBER, enhances lethality by improving Soldiers' physical, spiritual, and nutritional health, thereby boosting cognitive functions critical for cyber missions. A new NCO professional development plan incorporates H2F domains, recognizing that even non-physical roles benefit from optimized well-being.

Exercises like African Lion 2025 build readiness through multinational simulations, while the Cyber Battle Lab provides virtual environments for experimentation and gap identification. This proactive stance, combined with incentives for retention and recruitment, positions the workforce to counter escalating threats from adversaries.

Conclusion: A Force Primed for the Future

The U.S. Army's cyber workforce exemplifies a paradigm shift in military power, where lethality is defined by digital dominance, training by perpetual innovation, and readiness by holistic resilience. Through ARCYBER's leadership and programs like DCWF and H2F, this force not only defends against cyber threats but actively shapes the battlespace. As threats grow more sophisticated, the uniqueness of this workforce – rooted in technical expertise and adaptive strategies – ensures the Army remains lethal, trained, and ready in the cyber domain. ■

Aspect	Traditional Army Workforce	Cyber Workforce
Training Emphasis	Physical drills, marksmanship	Certifications, simulations, AI-enabled learning
Readiness Metrics	Deployment cycles, equipment status	Qualification rates, cognitive health KPIs, threat prediction

Engagement Skills Trainer

By Staff Sgt. Elliott Lefler, Operations Support Element

THE ARMY'S FOCUS ON LETHALITY, TRAINING, AND READINESS applies across every formation, whether kinetic or digital. While the tasks of a cyber professional look different from those of an infantry rifleman, the principles of preparation remain the same. Training must be realistic, repletion must build confidence, and readiness must be measurable.

Recently I took my Soldiers to the engagement skills trainer (EST) range. The goal was simple: reinforce the fundamentals of marksmanship through realistic, scenario-based training. The EST allows solders to build proficiency in a controlled environment before facing the stress of qualification or live fire. That investment in practice translates directly to battlefield confidence.

In many ways, this mirrors the preparation needed in the cyber domain. Most cyber Soldiers may not zero a weapon or fire at silhouettes, but they must sharpen their own fundamentals. Instead of target acquisition and trigger control, their skills involve analysis, troubleshooting, and problem-solving under pressure. Like the EST, cyber training environments provide the repetitions necessary to build instinctive responses before real-world missions.

Lethality in cyber is not about pulling a trigger; it is about ensuring the Army can operate, defend, and, when required, deliver effects in the information environment. This requires Soldiers who are confident in their technical abilities, just as riflemen are confident in their marksmanship. Both rely on training that develops trust in their skills and their teams.

Readiness, too, crosses domains. For infantry units, readiness is measured through weapons qualification, fitness, and deployment posture. For cyber units, it includes technical certifications, current in evolving tools, and the ability to adapt to emerging threats. While metrics differ, the underlying principle is the same: units must be prepared to fight.

It is also a reminder of shared responsibility. Leaders are charged with creating opportunities for training and development – whether that means time on the range or time in a cyber exercise. But it is equally the responsibility of junior Soldiers to take full advantage of those opportunities, to treat each repetition seriously, and to build habits that lead to confidence and competence when matter most.

The EST reinforced for my Soldiers that training is about more than passing a test. It is about building habits, sharpening fundamentals, and preparing for the stress of real-world execution. The same applies to the cyber force. No matter the domain – kinetic or digital – the Army remains committed to building lethal, trained, and ready Soldiers who can fight and win in any environment. ■

The Engagement Skills Trainer II (EST II) is designed to assist and improve the basic fundamentals of marksmanship, as well as collective and escalation of force training before going to a live-fire range. (Photo Credit: U.S. Army)

Cyber Lethality, Training, and Readiness: The Army's Digital Edge As cyber

By Pfc. Cedric Knight, Operations Support Element

AS CYBER THREATS BECOME MORE COMPLEX AND URGENT, the U.S. Army's capability to counter them is now vital to national defense. Cyber operations are playing more than a supporting role, they are a crucial element of our National Defense Strategy, with the ability to disrupt, disable, and destroy an enemy's capabilities without even firing a shot. In this dynamic field, the Army has developed a cyber force that is characterized by greater lethality, intense training, and high operational readiness – qualities necessary in guaranteeing dominance in the cyber and electromagnetic spectrum. This essay examines the unique aspects of cyber lethality, the Army's rigorous training regimens, and its focus on readiness, with particular emphasis on how these elements combine to ensure success in the ever-evolving arena of cyber warfare.

Lethality refers to the Army's ability to utilize cyber capability as a precision weapon, delivering strategic effects with long ranging consequences. Unlike traditional kinetic weapons, cyberattacks can infiltrate, degrade, and destroy an adversary's systems from within, and typically unnoticed. The lethal character of cyber war whether through the introduction of malware, denial of service, or manipulation of critical systems has revolutionized warfare in the contemporary period. For the Army, this represents a military doctrine revolution. The ability to shut down an enemy's communications grid, paralyze weapons systems, or even affect financial networks can have devastating effects without directly engaging. But that capability requires more than just powerful offensive tools; it requires a highly competent workforce that can think strategically and act with surgical precision. Army cyber warriors must be skilled in the full spectrum of cyber operations, from defensive cybersecurity to protect U.S. infrastructure to offensive techniques for exploiting adversary vulnerabilities. Offensive cyber operations, specifically, represent a new type of warfare one that is based on a combination of high-technology and planning and strategy. The Army's focus on cyber lethality has given rise to the creation of specialized cyber units, such as the U.S. Army Cyber Command (ARCYBER), which leads and executes sophisticated digital attacks as components of broader military operations. Cyber training is comprehensive, covering all domains of cybersecurity basics to sophisticated offensive and defensive operations. Army cyber workforce training goes beyond the typical IT certification and into the realm of real-world operations, adversary profiling, and mission planning.

- Technical Proficiency: Technical proficiency is at the core of Army cyber training. Soldiers undergo rigorous training in specialties that include network security, coding, ethical hacking, and digital forensics. This ensures that all cyber workforce members can find vulnerabilities in military and civilian networks, exploit weaknesses in enemy systems, and build secure networks that cannot be infiltrated by enemy cyberattacks.
- Simulations and Exercises: Unlike most traditional military operations, cyber exercises involve simulated environments where troops are subjected to situations that are akin to real world attacks. These live fire training events replicate large scale cyberattacks, including zero-day exploits, ransomware attacks, and intrusions into critical infrastructure. In these exercises, Army cyber Soldiers go through managing the uncertainty and rapid escalation that is characteristic of actual cyber warfare. These training programs are designed to simulate the dynamic, fluid environment of cyber warfare to allow Soldiers to think critically, to learn rapidly, and to respond to shifting circumstances with speed.
- Cross Disciplinary Training: What makes the Army's cyber training program unique is the cross-disciplinary approach. While cyber operations demand specialized technical skills, Army cyber Soldiers also learn military strategy, intelligence analysis, and coordination with other combat arms. For example, Army Intelligence officers work alongside cyber professionals so that cyber operations are led by accurate, timely intelligence. This allows the Army to create and conduct cyber operations more accurately, with a sense of both the technical and tactical terrain.
- Continual Professional Development: The rapidly changing nature of the cyber environment demands continuous professional development. The Army's training pipeline is not static; it is still evolving based on emerging threats, new technology, and lessons learned from previous operations. The incorporation of new technologies, such as machine learning and artificial intelligence, into Army cyber operations guarantees that training programs are updated continuously to keep Soldiers at the forefront of defense and attack methods.

Cyber readiness is critical to ensuring the Army's cyber force is poised to respond quickly and effectively to adversary threats. The cyber fight is 24/7, and the Army must be in a posture of constant readiness to address threats as they arise.

- Operational Integration: Readiness within the cyber force extends beyond training the individual to the integration of cyber capabilities into broader military operations. Army cyber forces must be able to support traditional forces in kinetic operations either by disabling an adversary's command and control systems or providing battlefield intelligence. The integration will ensure that cyber capability is not independent but well integrated into the Army's strategic objectives.

- Rapid Response Capability: The Army's cyber force must be prepared for rapid deployment at a moment's notice. Part of this preparedness is that Army cyber units train to operate in austere environments where they may not have immediate access to state-of-the-art facilities or support. This conditions Soldiers to conduct operations in numerous environments, from forward operating bases to joint command centers, so the cyber force remains agile and effective even in difficult circumstances.
- Inter-Branch Coordination: Army cyber operations do not function in isolation. They require the assistance of other branches of the military, from intelligence and special operations to logistics and aviation. The Army trains its cyber force to function across branches by conducting joint exercises and creating procedures for seamless integration. This coordination is specifically critical in advanced operations where cyber effects are synchronized with conventional warfare techniques.
- Resilience and Adaptability: The cyber domain is characterized by constant change, with threats modifying their tactics as quickly as defenses can be established. To this end, the Army's cyber workforce is built resilient and agile. Soldiers are not only trained to react to identified threats but are also trained to cope with new attacks and techniques. This mental agility ensures that Army cyber Soldiers can overcome even the most unexpected challenges.

As the nature of cyber threats continues to evolve, the U.S. Army must be at the forefront of cyber operations. The introduction of newer technologies like artificial intelligence, machine learning, and quantum computing into military cyber operations will add complexity to the cyber battlefield. These emerging technologies will demand even greater specialized training, along with greater coordination among Army cyber forces and the other military services. In the years to come, the Army's cyber operations will be further integrated into conventional military forces, enabling real time digital warfare to augment kinetic operations. The Army's ability to achieve precision strikes, protect critical infrastructure, and defend against cyberattacks and espionage will depend on its future investment in cyber readiness, training, and lethality.

Cyber operations represent a new frontier in modern warfare, and the U.S. Army's focus on developing a lethal, ready, and highly trained cyber force ensures its ability to secure dominance in the cyber domain. By combining technical expertise, cross-functional training, and inter branch collaboration, the Army's cyber force is well positioned to carry out focused, high impact operations against adversaries. The Army's emphasis on readiness and agility ensures its cyber warriors remain a step ahead of the next challenge, regardless of the speed at which the cyber landscape evolves. With cyber lethality at its core, the Army is leading the way in shaping the future of warfighting in the era of the digital age.

Army Principal Cyber Advisor Visits U.S. Army's Only Offensive Cyber Operations Brigade

***FORT GEORGE G. MEADE, Md.** – The U.S. Army's principal cyber advisor to the Secretary of the Army, Mr. Brandon Pugh, visited the 780th Military Intelligence Brigade (Cyber) – the Army's only offensive cyber operations brigade, August 6.*

FORT GEORGE G. MEADE, MD – Mr. Brandon Pugh, the U.S. Army's Principal Cyber Advisor to the Secretary of the Army, visited the 780th Military Intelligence Brigade (Cyber) on August 6. The brigade is the Army's sole offensive cyber operations unit, playing a pivotal role in national defense and cyber warfare.

The visit followed Mr. Pugh's three-day trip to U.S. Army Cyber Command (ARCYBER) headquarters at Fort Gordon, Georgia, where he received briefings and engaged directly with ARCYBER's top talent.

"The 780th Military Intelligence Brigade (Cyber) is on the frontline of defending our nation and conducting cyber operations," said Brandon Pugh, the Army's Principal Cyber Advisor. "The brigade is an invaluable component of the United States' cyber enterprise. My visit to the 780th Military Intelligence Brigade (Cyber) was an extraordinary opportunity to meet Soldiers conducting these important cyber operations and to see its unique capabilities firsthand."

During his time in Georgia, Mr. Pugh met with capability developers from the 11th Cyber Battalion, who showcased innovative, in-house engineered devices tailored to meet the operational needs of expeditionary cyber teams. He also interacted with Soldiers from the 782nd Military Intelligence Battalion (Cyber), who support Cyber Joint Force Headquarters (JFHQ-C) for the Army, Air Force, Navy, and Marine Corps.

The 780th MI BDE (Cyber) is geographically dispersed across four states. The brigade headquarters, the 781st MI Battalion (Cyber), and the Operations Support Element (OSE), are based at Fort George G. Meade, Maryland; the 11th CY Battalion and 782d MI Battalion (Cyber) are headquartered at Fort Gordon, Georgia; and the 782d has operational detachments in Hawaii and Texas.

According to the Brigade commanding officer, Col. Candy Boparai, the 780th MI BDE (Cyber) is a critical enabler of ARCYBER and U.S. Cyber Command (USCYBERCOM), delivering unique, multi-domain capabilities to sense, understand, and deliver effects in the information environment.

"The 780th MI Brigade (Cyber) directly supports USCYBERCOM's core missions: defending the Nation and conducting cyber operations to achieve Combatant Command objectives," said Boparai. "We operate as a key component of the Army's Cyber Mission Force (CMF), specifically providing National Mission Teams, National Support Teams, Combat Mission Teams, and Combat Support Teams, and Capability Solutions Developers."

According to Command Sgt. Maj. Joseph Daniel, the brigade's senior enlisted leader, "As the Army's only offensive cyber force, the 780th provides unique capabilities to sense, understand, and deliver tactical, operational and strategic cyber effects globally to achieve Combatant Command objectives."

Daniel remarked that the brigade supports Joint Force efforts, leveraging their more than 2,100 personnel to address cyber challenges worldwide; and the brigade's cyber teams, 11th CY BN Expeditionary CEMA (cyberspace electromagnetic activities) Teams (ECTs), and developers are all actively involved in regular cyber operations, collaborating with USCYBERCOM, Army electronic warfare units, and other partners.

In addition to receiving briefings, Mr. Pugh was able to see a live operation in the brigade's Joint Mission Operations Center and view an Army Continuous Transformation drone demonstration by the OSE Cyber Solutions Development team.

As part of the Principal Cyber Advisor's briefing, the brigade discussed the training requirements to achieve and maintain mastery in a Cyber Soldier's assignment. These requirements are executed at the brigade, following their training at the U.S. Army Cyber School. The additional training can range from several months to more than a year and continues as the Soldiers progress.

"The Army's most significant inputs into cyber readiness are presenting high quality personnel and providing the supporting talent management policies to sustain them in Cyber Mission Force long enough to achieve and maintain mastery in their skillsets," said Boparai. "We are the only U.S. Army offensive cyber operations brigade and our focus as the administrative command headquarters is to man, train, equip, assess and enable the Army CMF and CEMA teams in accordance with published USCYBERCOM and ARCYBER standards."

The 780th MI Brigade (Cyber) motto is inscribed on the organization's Distinctive Unit Insignia "Ubique Et Semper In Pugna." Latin for "Everywhere and always fighting," we don't specifically talk about what we do nor who we are in a cyber 'knife fight' with; however, we are *"Everywhere and Always...In the Fight!"* ■

***FORT GEORGE G. MEADE, Md.** – In addition to receiving briefings, Mr. Pugh was able to see a live operation in the brigade's Joint Mission Operations Center and view an Army Transformation Initiative drone demonstration by the Operations Support Element's Cyber Solutions Development team.*

The Unique Lethality of the Cyber Workforce: Language, Training, and Readiness in the 35P Community

By Staff Sgt. Kyle Freshwater, BDE S3, 780th MI Brigade (Cyber)

THE ARMY'S CONCEPT OF LETHALITY often conjures images of tanks, rifles, and artillery. But in the modern era, lethality stretches beyond the kinetic battlefield. In the cyber domain, information is both a weapon and shield, and readiness depends as much on mastery of language and communication as coding or network defense… or even more so. This is where the 35P Cryptologic Linguist or Signals Intelligence Voice Interceptor plays a vital role (depending on when one joined).

Lethality in Language

Unlike other domains, cyber operations are global in scope and instantaneous in effect. Success often depends on anticipating, detecting, and neutralizing threats before they manifest. For 35Ps, lethality comes not from pulling a trigger, but from understanding adversary intent in real time. This is one of our core competencies that we contend with daily. Language is our weapon. A skilled linguist can detect nuance, intent, and deception in communication that no machine can replicate. To do this, a linguist must master idioms, cultural context, and unspoken rules to deliver timely and accurate intelligence.

But what does that mean for the cyber domain? What does a 35P really provide for the fighting force? Commanders and colleagues often ask, "What is it that you do?" From the outside looking in, it is a fair question. Too frequently, the quick answer is, "Oh, we do language." But that answer does not even scratch what a 35P brings to combat power. My favorite way to answer now is with a quote from a mentor: "We define the infinite."

In Army terms, 35Ps are more than linguists; we are culture, language, translation, and interpretation experts. We must understand a culture in depth, its nuances, concepts, and idioms. We must master the rules and associations of language. We must be able to produce professional translations, deliver accurate transcripts, and interpret in real time under pressure. And as a reminder, we are also SIGINTers (signals intelligence). Language is one of our weapons, but it is only one part of a larger arsenal. Our work sits at the intersection of language and signals intelligence, where words, data, and context combine into actionable combat power.

On the surface, this might sound straightforward, but it is not. What exactly is a "professional transcript"? How do you define a "culture"? In cyberspace, each forum, chat room, or blog can be its own culture, with written and unwritten rules, slang, and inside references. As 35Ps, we are expected to recognize and move across all of them.

This is where language theory aligns with what we do in practice. Schleiermacher once said a translator either moves the reader closer to the foreign text or the text closer to the reader. That is the same balancing act we face every day. Sometimes, we preserve the exact words and keep the foreignness, so analysts see what the adversary said. Other times, we adapt it so a commander can understand the meaning in a split second. Both choices are part of readiness.

Anthony Pym put it another way: translation is cooperation and risk management. That is also our world. Every time we interpret or translate under pressure, we manage risk, decide how to handle ambiguity, how much context to give, and what will best keep the force ahead of the threat. Readiness means being sharp enough in our language and cultural knowledge to make those calls when it matters.

What is Readiness for 35Ps

What does readiness look like for a 35P in a cyber unit? Is it the same as professionalization? Are 35Ps expected to be as trained on systems as their 17C counterparts? In my view, the answer to all of those is yes. Readiness starts with proficiency. The Defense Language Proficiency Test (DLPT) does precisely what its name says: it tests language proficiency. It takes 36 to 64 weeks of training just to sit for that test. That is the baseline, renewed yearly or biannually depending on your score. But that baseline is not the finish line. Readiness means continuous training, language training, culture training, and constant practice. Cultural intelligence comes through exposure, and for us, that exposure ties directly to language. Every lesson builds not just words, but an understanding of the people and the mindset behind them.

Readiness also means integration. We are not only linguists, but we are also SIGINTers. That means applying our language skills in the full spectrum of signals intelligence: intercept, collection, analysis, and reporting. A transcript or translation does not live in isolation; it ties to technical systems, data, and the bigger picture of the mission. A 35P who is only "good at language" is not fully ready. Actual readiness is being able to sit next to a 17C, understand the system they are operating on, and provide the language and cultural layer that makes the signal actionable. Our value is in fusing language with SIGINT to deliver intelligence that commanders can act on in real time.

Finally, readiness is holistic. We cannot separate being a linguist from being a Soldier. Continuous training is not just about keeping our DLPT scores up; it is also about staying fit, qualified, and mentally sharp. The cyber fight does not excuse us from ruck marches, weapons qualification, or physical readiness. Instead, it demands more. A 35P must be able to translate a message under pressure, analyze it within the SIGINT framework, and maintain the discipline and toughness expected of any Soldier in the Army. That blend of language, SIGINT integration, and Soldier readiness is what makes our role unique and what makes us lethal in the cyber domain.

Conclusion

The Army often measures lethality in rounds fired or targets destroyed. Still, in cyberspace, measure of lethality is in what never happens: the attack that never materializes, the misinformation campaign that never takes hold, the adversary plan that never reaches execution. For 35Ps, our weapon is language. Our training in culture, idioms, and nuance allows us to turn intercepted signals into intelligence that protects the force and gives commanders the edge. Readiness for a 35P is not just about the DLPT, training, SIGINT, and holistic Soldier readiness. It is about sitting next to our cyber operators and analysts and adding the "so what" and at a depth that no system can replicate.

This makes the 35P unique within INSCOM, USCYBERCOM, and ARCYBER. No other force blends language, cultural intelligence, and SIGINT expertise the way we do. With that perspective in mind, this organization has a unique advantage, the unmatched capability to anticipate, disrupt, and neutralize threats before they ever hit the battlefield. What makes the 35P unique is our ability to bridge worlds, between languages, cultures, and between humans and technology. That ability alone describes our lethality and gives credence to our readiness.

Bibliography:

[1] Pym, A. (2014). *Exploring translation theories* (2nd ed.). Routledge. Schleiermacher, F. (1813/2012). *On the different methods of translating*. In L. Venuti (Ed.), *The translation studies reader* (3rd ed., pp. 43–63). Routledge.

[2] U.S. Army Cyber Command (ARCYBER). (n.d.). *About U.S. Army Cyber Command*. Retrieved from https://www.arcyber.army.mil

[3] U.S. Cyber Command (USCYBERCOM). (n.d.). *About U.S. Army Cyber Command*. Retrieved from https://www.arcyber.army.mil

[4] U.S. Army Intelligence and Security Command (INSCOM). (n.d.). *Mission and vision*. Retrieved from https://www.inscom.army.mil

[5] Defense Language Institute Foreign Language Center (DLIFLC). (n.d.). *Defense Language Proficiency Test (DLPT)*. Retrieved from https://www.dliflc.edu_

11th Cyber Battalion Change of Command

By Cpl. Teanna Dooley, 11th Cyber Battalion

FORT GORDON, Ga. – Soldiers, Civilians, friends and family bade farewell to Lieutenant Colonel Luis (Lou) A. Etienne, the outgoing commander of the 11th Cyber Battalion, Leviathans, and welcomed Lt. Col. Charles E. Suslowicz, their new battalion commander, in a ceremony hosted by Colonel Candy Boparai, commander, 780th Military Intelligence Brigade (Cyber), on Barton Field, June 25. In a ceremony steeped in Army tradition, Soldiers representing the Headquarters and Headquarters Company, Hellhound; A Company, Apex; B Company, Bandits; and C Company, Capybara, stood in formation to pay their respects to both the outgoing and incoming battalion commanders.

"This is no ordinary formation. The 11th Cyber Battalion's mission is unlike any mission in the Army. They are charged with answering a question that the DoD (Department of Defense) is still grappling with, 'what does tactical CEMA (Cyberspace Electromagnetic Activities) mean on tomorrow's battlefield.' Building a unit is hard enough, but building a concept of employment for the entire Army is harder yet," said Col. Boparai. "To the Soldiers of this unit, Leviathans, make no mistake, what you're building here is consequential. You're shaping not just how we fight, but how we think about fighting in unchartered territory. Your resolve, your professionalism, have been constant and noted."

Lt. Col. Lou Etienne has built a distinguished military career across infantry, intelligence, and cyber operations. He led combat operations in Iraq and Afghanistan and later transitioned into cyber warfare, where he commanded Cyber Protection Teams and held dual leadership roles within the Cyber National Mission Force. He holds advanced degrees, completed Senior Service College, and earned prestigious badges including the Ranger Tab and Combat Infantryman's Badge – hallmarks of operational excellence and leadership.

"Through all of this change and all of the challenges, and the opportunities 11th Cyber has had, Lou's leadership has steered this team through uncertainty and towards clarity," said Col. Boparai. "Lou, you led during a time when there was no playbook, there was just potential, and you gave your Soldiers the confidence to explore that potential. Your vision and commitment and passion for this unit, your love for this unit, really set the groundwork for what this unit has become, and your impact will be felt long after (the battalion colors have) changed."

Lt. Col. Etienne was recognized for his outstanding service and unwavering dedication to the mission. The unit extends its deepest appreciation for his leadership and contributions and wishes him continued success in all future assignments.

"I've learned that any success that I have as a leader in the Army will only happen if my Soldiers are taken care of and if my Soldiers have purpose," said Lt. Col. Etienne. "In the past few days, I received many messages of congratulations on a successful command. My response is always the same. My success is due to the amazing work done by each and every one of the individuals you see before you, along with individuals of the battalion who could not be here today."

Etienne listed a few of the Levithan successes and contributions, including: driving LMTVs (Light Medium Tactical Vehicle) and delivering food and supplies to garrison residents after Hurricane Helene; maneuvering Expeditionary Firing Crews during CTC (Combat Training Center) rotations demonstrating CEMA at the tactical cyber edge; winning the Army Cyber Command Best Squad Competition (BSC) two years in a row and last year, going to the Army BSC, and beating out special operations, infantry, and armor commands with a squad of cyber warriors, EW (electronic warfare) warriors, and a mechanic; developing ground breaking radio frequency-based capabilities that would change the targeting paradigm for tactical maneuver formations in the Army and Joint force; and teaching cyber and networking fundamentals to high school students at Richmond County Technical Career Magnet School, the battalion's adopted school.

"(I) just led the amazing Soldiers who did do all that and so much more," said Lt Col. Etienne. "I woke up every day during that last two years of my command knowing I had to give my 110 percent effort because I never wanted to let any of my Leviathan brothers and sisters down, and as I gracefully bow out of command, I only hope that you all understand the gratitude I have for all the hard work and commitment to each other and our mission. Thank you, Leviathans, for the best two years of my career."

Lt. Col. Charles Suslowicz has cultivated a remarkable professional journey spanning signal, cyber, and academic roles. He led communications operations in support of Operation Enduring Freedom and helped pioneer the establishment of the Army's Cyber Protection Teams. His contributions as a research scientist and professor at West Point underscore his commitment to advancing cyber capabilities and education. With leadership roles at the Army Cyber Institute and Cyber National Mission Force, and advanced degrees in engineering, he exemplifies technical expertise and visionary service.

"This unit is proof that our Army can evolve and innovate in every domain, and the mission ahead will continue to be demanding and unconventional, but I have every confidence that the future of tactical cyber is in the best possible hands," said Col. Boparai.

Lt. Col. Suslowicz's comprehensive background in operational, academic, and cyber leadership reflects the caliber of experience expected of a battalion commander. His appointment as the 11th Cyber Battalion commander highlights his exceptional qualifications and steadfast dedication to mission success.

"To the Soldiers of the 11th. Thank you for all that you've done and for all that you're going to do. I saw how amazing you were in the last few years, from afar, over at the 780th headquarters at Fort Meade, and in the last few weeks you demonstrated how truly incredible you are as I got to know just a few of you as I'll get to know the rest of the Soldiers in this formation in the coming days and weeks," said Suslowicz. "This is going to be great!
Global Reach,
Global Impact!
Leviathan 6 signing on". ■

FORT GORDON, Ga. *– Col. Candy Boporai, commander for the 780th Military Intelligence Brigade Commander, hosted a change of command ceremony whereby Lt. Col. Luis (Lou) A. Etienne, relinquished his command of the 11th Cyber Battalion, Leviathans, to Lt. Col. Charles (Chuck) E. Suslowicz, on Barton Field, June 25.*

The passing of the colors during a U.S. Army change of command ceremony symbolizes the formal transfer of authority, responsibility and accountability from the outgoing commander to the incoming one, reinforcing the continuity of leadership and the unit's enduring legacy. (U.S. Army photos by Sgt. 1st Class Kyle Alvarez) .

Cyber Legion Change of Command Ceremony

By 1st Lt. Jonathan Daugherty, 782d Military Intelligence Battalion (Cyber)

FORT GORDON, Ga. – The 782d Military Intelligence Battalion (Cyber), Cyber Legion, marked a significant transition of leadership during a change of command ceremony held on Barton Field, June 4.

Senior Leaders, family, friends, and Soldiers of the Cyber Legion gathered to bid farewell to outgoing commander, Lt. Col. Kirklin Kudrna, and welcomed the incoming commander, Lt. Col. Matthew Hutchison. The ceremony, steeped in tradition, formally transferred responsibility for the unit's vital cyber mission, ensuring continued readiness and dominance in the information environment. Presiding over the event was the commander of the 780th MI Brigade (Cyber), Col. Candy Boparai, who lauded Lt. Col. Kudrna's leadership and expressed confidence in Lt. Col. Hutchison's ability to lead the 782d MI BN forward.

During Lt. Col. Kudrna's tenure, the 782d MI BN consistently exceeded expectations in support of national security objectives, notably enabling two new Cyber Mission Force teams to reach Full Operating Capacity and developing a brand-new training scenario for mission readiness events. He skillfully navigated the complexities of the rapidly evolving cyber landscape, fostering a culture of innovation and resilience within the ranks. He expressed deep gratitude for the dedication and professionalism of the Soldiers and Civilians who served alongside him, emphasizing their contributions to the unit's successes.

Lt. Col. Hutchison assumed command, bringing with him a wealth of experience in cyber operations and a proven track record of leadership and success. He previously served as Chief of Strategic Initiatives, U.S. Army Cyber Command (ARCYBER).

During the ceremony, Lt. Col. Hutchison addressed the assembled Soldiers conveying his excitement and dedication to leading the 782d MI BN.

"I'm honored and excited to join this Battalion and to be a part of the illustrious 780th Military Intelligence Brigade," Lt. Col. Hutchison remarked. "While serving in the Cyber Protection Brigade and at ARCYBER, I've long heard the tales and exploits of the Cyber Legion. Today's current operating environment gives cyber forces little respite from the stresses of sustained training and operations. However, I look forward to working as a team to pursue mastery in our craft and continuing to take measured steps to be the most well-trained and adaptable cyber forces supporting the Joint Force."

The change of command concluded with a reception, allowing attendees to personally congratulate both Lt. Col. Kudrna and Lt. Col. Hutchison.

The 782d MI BN stands poised to continue its critical mission under Lt. Col. Hutchison's leadership, safeguarding national interests in the digital realm. The unit looks forward to building upon the strong foundation laid by Lt. Col. Kudrna and embracing the challenges and opportunities that lie ahead. ■

***FORT GORDON, Ga.** – Col. Candy Boparai, commander, 780th Military Intelligence Brigade (Cyber) hosted a change of command ceremony on Barton Field whereby Lt. Col. Kirklin Kudrna relinquished his command of the 782nd Military Intelligence Battalion (Cyber), Cyber Legion, to Lt. Col. Matthew Hutchison, June 4. (U.S. Army photo by Sgt. 1st Class Kyle Alvarez)*
Cyber Legion… Silent Victory.

11th Cyber Battalion NCO Induction Ceremony

By Cpl. Teanna Dooley, IT Specialist, 11th Cyber Battalion

FORT GORDON. Ga. – The 11th Cyber Battalion held its first Noncommissioned Officer (NCO) Induction Ceremony, celebrating the advancement of Soldiers from junior enlisted to Noncommissioned Officers, at the Gordon Conference Center, August 21, 2025.

The NCO Induction Ceremony marks a significant milestone in the careers of its newly promoted leaders. These NCO leaders are entrusted with maintaining discipline, enforcing standards, and safeguarding the well-being of their fellow Servicemembers. The ceremony recognized inductees from Headquarters, Alpha, and Charlie Companies:

- Headquarters Company: Sgt. Santonio Andrews, Sgt. Jayden Brinkerhoff, Sgt. Landar Fangsrud, Sgt. Pedro Felix, Sgt. Daniel Kim, Sgt. Julyana Macedo, Sgt. Darrious Mccoy, Sgt. Aiden Murphy, Sgt. Essence Willis
- Alpha Company: Sgt. Conner Allsup, Sgt. 1st Class Brandon Bozant, Sgt. Issac Johnson, Sgt. Mason Miller
- Charlie Company: Sgt. Joshua Boynton, Sgt. Tyler Imhoff, Staff Sgt. Isiah Nembhard, Sgt. Jospeh Ramos, Sgt. Andrew Sliter

Command Sgt. Maj. Timothy McGuire, the senior enlisted leader of the U.S. Army Cyber Center of Excellence, served as the guest speaker, delivering a powerful message drawn from his 27 years of being a Noncommissioned Officer.

"The title of Noncommissioned Officer isn't given; it's earned," said McGuire.

He emphasized that the role carries immense responsibility, not only in technical expertise but in leadership and mentorship.

McGuire left the inductees with three core duties:

1. Be experts in your craft – Maintain technical proficiency while leading.
2. Know and enforce standards – "If you don't enforce the standard, your lack of enforcement becomes the standard."
3. Take care of your soldiers – Support, train, and prepare them for mission success.

Reflecting on his own journey, McGuire shared stories of early challenges, leadership lessons, and the importance of treating soldiers with dignity and respect. He reminded the audience that leadership is not just NCO business, it's leader business.

As the ceremony concluded, the inductees stood ready to lead, uphold the Army's values, and carry forward the legacy of the Noncommissioned Officer.

Global Reach, Global Impact! ■

NCO Corps
Rite of Passage

U.S. Army Cyber Command Best Squad Competition 2025

FY25 ARCYBER SOLDIER OF THE YEAR
FY25 ARCYBER NCO OF THE YEAR

***FORT HUACHUCA, Ariz.** – After a challenging and action-packed week in April at the U.S. Army Cyber Command Best Squad Competition, congratulations to all the outstanding Soldiers who gave it their all — and a special shoutout to the winners who rose to the top:*

ARCYBER's Best Squad: 11th Cyber Battalion
ARCYBER's Top NCO: Sgt. Buckwalter, 11th Cyber Battalion
ARCYBER's Top Soldier: Spc. Robey, 11th Cyber Battalion
Your hard work, dedication, and warrior spirit truly stood out. Well done to all!

11th Cyber Battalion
Best Squad

WASHINGTON, D.C. *- U.S. Army soldiers with the 11th Cyber Battalion, 780th Military Intelligence Brigade, Army Cyber Command, participate in a fitness competition during the Army's 250th Birthday Festival in Washington, D.C., June 14, 2025. The event highlights physical readiness as a core Army value and a key component of building resilient, mission-ready Soldiers. (U.S. Army photo by Spc. Eric Vicenty, 55th Public Affairs Company Combat Camera)*

WASHINGTON, D.C. *- U.S. Army Spc. Martin Dyhhon, with the 11th Cyber Battalion, 780th Military Intelligence Brigade (Cyber), Army Cyber Command, participated in a fitness competition during the Army's 250th Birthday Festival in Washington, D.C., June 14, 2025. The event highlights physical readiness as a core Army value and a key component of building resilient, mission-ready Soldiers. (U.S. Army photo by Spc. Eric Vicenty, 55th Public Affairs Company Combat Camera)*

WASHINGTON, D.C. *– U.S. Army Soldiers assigned to the 11th Cyber Battalion, 780th Military Intelligence Brigade, Army Cyber Command, participate in the Army Fitness Competition in Washington D.C. in honor of the Army's 250th Birthday Parade, June 14, 2025. The U.S. Army's 250th Birthday Celebration will honor the sacrifices, achievements, and enduring spirit of American warriors through a fitness competition, festival, and parade—offering the public an opportunity to engage with Soldiers, Army astronauts, NFL representatives, and Medal of Honor recipients.(U.S. Army photo by Sgt. Macaydan Hawkins, 55th Public Affairs Company Combat Camera)*

EST. 1775
250
U.S. ARMY
THIS WE'LL DEFEND

Happy 250th Birthday U.S. Army!

FORT GEORGE G. MEADE, Md. *– Soldiers representing the 780th Military Intelligence Brigade (Cyber), Praetorians, including the Brigade Headquarters and Headquarters Company, Hastati, 781st MI Battalion (Cyber), Vanguard, and Operations Support Element, participated in the Garrison Army 250 Birthday Run, June 13.*

"This We'll Defend"

INSCOM Senior Leader visits 11th Cyber Battalion!

***FORT GORDON, Ga.** – Command Sergeant Major (CSM) Anthony "Tony" Rangel III, the senior enlisted leader for U.S. Army Intelligence and Security Command (INSCOM), received a capabilities brief from the Soldiers of the 11th Cyber Battalion.*

During his visit to the 11th CYB, CSM Rangel had the opportunity to engage directly with the Soldiers and gain firsthand insights into the impact of the Small Unmanned Aerial Systems (SUAS) program on operational readiness.

The visit was a resounding success, reinforcing the SUAS program's value and laying the foundation for enhanced collaboration with INSCOM leadership. The innovation of the battalion's Soldiers is indicative of the Army Transformation Initiative.

HHC, 11th Cyber Battalion, Change of Responsibility Ceremony

FORT GORDON, Ga. *– Soldiers representing Headquarters and Headquarters Company, 11th Cyber Battalion, bade a fond farewell to the outgoing first sergeant and senior enlisted leader, 1st Sgt. James Kennedy, and welcomed 1st Sgt. Timothy Nicholas, in a change of responsibility ceremony hosted by Capt. Cutosha Dilworth, the company commander, June 10.*

(U.S. Army photo by Army Capt. Angeline Kinser, B Co., 11th Cyber Battalion)

D Company, Operations Support Element, Change of Command Ceremony

FORT GEORGE G. MEADE, Md. – Soldiers and Civilians representing D Company, Operations Support Element (OSE), Delta Daemons, bid farewell to their outgoing company commander, Capt. Kenneth C. McGaffey, and welcomed their incoming company commander, Capt. Madeleine M. Schneider, in a change of command ceremony hosted by Lt. Col. Michael B. Krogh, the OSE commander, at the MG DeKalb Army Reserve Center, June 13.

Praetorian Soldiers graduate from the U.S. Army Advanced Leader Course

FORT GEORGE G. MEADE, Md. – *Staff Sgt. (SSG) Jonathan Quezado Ocampo was on the Commandants List and SSG Mathew Peterson, both assigned to the Brigade S3 Training section, 780th Military Intelligence Brigade (Cyber), Praetorians, graduated from the U.S. Army Advanced Leader Course (ALC), a branch-specific resident phase where Soldiers focus on the skills needed to lead squad- and platoon-sized units, June 25.*

Cyber Soldiers visit Blythe Summer Camp: July 17, 2025 Blythe, Ga

*FORT GORDON, **Ga.** – Soldiers from the U.S. Army Cyber Command at Fort Gordon, all members of the Sergeant Audie Murphy Club, spent time with youth ages 5 to 11 during a summer camp session at the Blythe Area Recreation Center, July 17. They shared their Army experiences and responded to a wide range of camper questions — from favorite foods to video games and more, all sparked by youthful imagination. The visit was part of a community outreach effort and ended with plenty of smiles all around. (U.S. Army photos by David Logsdon)*

Praetorians graduate from Army Ranger School –
RANGERS LEAD THE WAY!

FORT BENNING, Ga. *– Officers from the 780th Military Intelligence Brigade (Cyber), Praetorians, recently graduated from the U.S. Army Ranger School.*

Ranger School is one of the toughest training courses for which a Soldier can volunteer. Army Rangers are experts in leading Soldiers on difficult missions — and to do this, they need rigorous training. For more than two months, Ranger students train to exhaustion, pushing the limits of their minds and bodies.

1st Lt. Nathan Vowinkel graduated from Ranger School and earned his tab on August 8; and 1st Lt. Trevor Powers graduated in June.

The purpose of the Army's Ranger course is to prepare these Army volunteers — both officers and enlisted Soldiers — in combat arms related functional skills. The Rangers' primary mission is to engage in close combat and direct-fire battles.

Congratulations!

RANGERS LEAD THE WAY!

PRAETORIANS

Cyber Branch at West Point Branch Week

WEST POINT, N.Y. – Office Chief of Cyber with support from Army Cyber Institute, 780th MI (Cyber) Brigade, Cyber Protection Brigade, 82nd Airborne Division, and 75th Ranger Regiment is at West Point Branch Week 25-30 August.

Officers and enlisted personnel are informing cadets about the critical role Cyber and Electromagnetic Warfare plays in enabling operations at every echelon across all components!

Cadets were excited to engage these cyber professionals on what to expect in BOLC and their first duty station. They were especially interested in seeing the tactical mounted and dismounted systems at the tent this year. Many cadets were glad to hear that branch detail was an option, gaining tactical experience in either Air Defense Artillery, Field Artillery, Armor, or Infantry during their Lieutenant years and coming back to attend Cyber Captains Career Course.

Go Cyber!

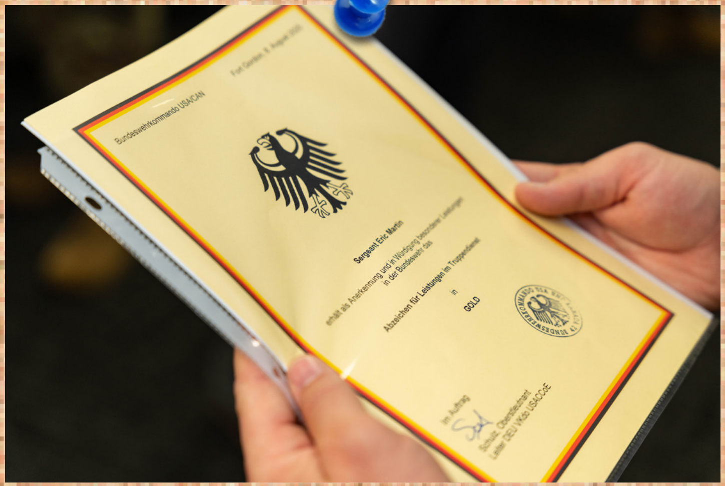
25th Infantry Division Patching Ceremony

SCHOFIELD BARRACKS, Hawaii *– U.S. Army Hawaiʻi and the 25th Infantry Division held a Shoulder Sleeve Insignia Patching Ceremony at Weyand Field, continuing a decades-long tradition of welcoming new Soldiers to Hawaii, June 2.*

Detachment Hawaii, 782nd Military Intelligence Battalion (Cyber) leaders, Soldiers, and the Soldier's sponsors welcomed Privates Frist Class Griffy, Jimenez, King, Sandoval, and Williams, presenting the new Soldiers with leis and "patching" their uniforms with the 780th MI Brigade unit patch. DET-HI extends the warmest aloha to our new Soldiers and their families!

(U.S. Army Photos by 1st Lt. Leo Ras, DET-HI)

German Armed Forces Badge for Military Proficiency Graduation



Bundeswehrkommando USA/CAN

Fort Gordon, 8. August 2023

Sergeant Eric Martin

erhält als Anerkennung und in Würdigung besonderer Leistungen in der Bundeswehr das

Abzeichen für Leistungen im Truppendienst

in

GOLD

BUNDESWEHRKOMMANDO USA UND KANADA

Im Auftrag

Schulz, Oberstleutnant
Leiter DEU VKdo USACCoE

__FORT GORDON, Ga.__– Soldiers from the 11th Cyber Battalion received either the bronze, silver or gold German Armed Forces Proficiency Badge (GAFPB) based on their performance in completing the five required GAFPB events: a CLS test; basic PT test; swim test in uniform; 12k ruck march; and pistol marksmanship, in the NCOA RDL Conference Room, August 8.

Of the six Soldiers to receive the GAFPB, two received the bronze GAFPB; one the silver GAFPB; and three Soldiers received the gold GAFPB.

NEXT QUARTER'S BYTE IS focused on the Brigade's Warrant Officers. 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 November 15, 2025. Final articles are due November 29.