780th MILITARY INTELLIGENCE BRIGADE (CYBER)

THE BYTE

Vol. 14, Issue 4
October 2026



THE ARMY AZIMUTH:
Outpace Our Adversaries

PRAETORIANS

780th MI BDE
"STRENGTH AND HONOR"

COL Benjamin Klimkowski
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.

The Road Ahead on Outpacing Our Adversaries at the Technical Edge 1
COL Klimkowski, CDR, 780th MI BDE

The Army Azimuth 3
GEN Christopher C. LaNeve, VCSA

LaNeve: Army Must Outpace Adversaries, Ensure Dominance 4
Association of the United States Army

Intel Support to Cyber: *A quick look at the CMIG and other observations* 5
CW4 (Ret.) Michael Lewis, former STA, 781st MI Bn

Who Am I? Why Am I Here? 8
SGT Jonathan Villarreal, C Co, 781st MI Bn

Vanguard Food Drive 9

Facing Complexity: *Three Principles to Help Cyber Leaders Adapt their Organizations* 11
MAJ Bryan Reasonover, DET-TX, 782d MI Bn

Lethality in the Spectrum: *Transforming Expeditionary Electromagnetic Warfare for Future Combat* 13
CPT Christopher Priestly, DET-HI, 782d MI Bn

Outpacing the Adversary: *How AI Enables Decision Dominance in Cyberspace* 15
CPT Teisha Hardin, Cyber, 102 CST Lead, 782d MI Bn

11th Cyber Warfare Battalion: *2026 Edition* 17
CPT David Kim, CEMA Planner, 11th CWBn

RIFT: Forging Readiness Before Qualification 20
1SG Timothy Nicholas, HHC, 11th CWBn

Applying Cyber Fires in the Right Place at the Right Time 23
CPT Tate Bowers, OSE, 780th MI BDE

Adversary AI: *How US Cyber Command is Adapting to the New Digital Battlefield* 25
PFC Ian Bortoluzzi, OSE, 780th MI BDE

Bandwidth, Power, and the Core Host 27
CH Christopher Schafer, BDE Chaplain,
780th MI BDE

780th Military Intelligence Brigade (Cyber) Change of Command Ceremony 29
780th MI BDE

AvengerCon X is a Wrap for 2026 33
780th MI BDE

Some Retirement Remarks from CW4 Michael Lewis, former Vanguard Senior Technical Advisor 37

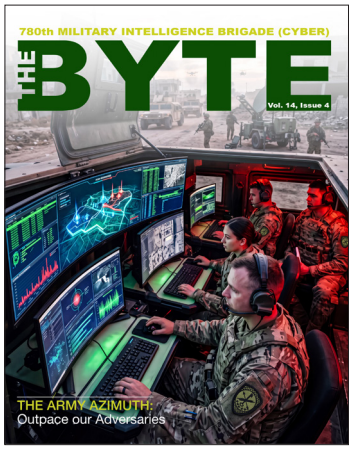
HHD (Herculians), Operations Support Element Change of Command ceremony 39

HHC, 780th MI Brigade (Cyber), Hastati, Change of Responsibility Ceremony 40

B Company (Immortals), 781st MI Battalion (Cyber) Change of Command ceremony 41

Brigade Suicide Prevention Hike 42

Praetorians organize and participate in Royal Danish Air Force March 43



On the Cover
Genrated By AI



FROM THE EDITOR:
COL Benjamin Klimkowski, Praetorian 6, took command of the 780th Military Intelligence Brigade (Cyber) on July 14, 2026. He is the ninth Praetorian Commander, and shortly after he took command provided me with his vision for his public affairs program. He tasked the brigade public affairs officer (PAO) and executive officer to develop a public affairs strategy that clearly outlines our long-term engagement plan and provides a guiding vision to underpin all our public affairs endeavors, and he provided two central foci to underpin his intent for this strategy:

Recruitment Focus: *We must find ways to project our message to the American public, enhancing our ability to attract and recruit top-tier civilian talent who desire to serve their country.*

Academic/Professional Focus: *We want to preserve and reinforce The BYTE magazine as a vehicle for professional stewardship within our formation—serving as a forum for us to discuss and advance the cyber profession.*

Praetorians, the Brigade Commander just provided his commander's intent for his public affairs program. *The BYTE* isn't my magazine. It's your magazine – and his vision for *The BYTE* is to "discuss and advance the cyber profession."

Let's get to work.

"Ubique Et Semper In Pugna"
"Everywhere and Always…In the Fight!

Steve Stover
Public Affairs Officer,
780th MI BDE (Cyber)
Editor, *The BYTE*

The Road Ahead: *Outpacing Our Adversaries at the Technical Edge*

By COL Benjamin H. Klimkowski, Commander, 780th Military Intelligence Brigade (Cyber)

IN THIS EDITION OF *THE BYTE*, our focus is squarely on "Outpacing Our Adversaries." In his strategic direction to the force, "The Army Azimuth," the Vice Chief of Staff of the Army established a clear bearing for our enterprise: we must aggressively transform, modernize, and sharpen the Force to prevail in high-intensity, multi-domain conflict. We stand at a historic inflection point where disruptive, accelerating technologies challenge established military practices and doctrine. As a cutting-edge, highly technical formation, the 780th Military Intelligence Brigade (Cyber) serves as the vanguard driving Army modernization, integrating technical capabilities, and projecting combat power across all echelons in the land domain, cyberspace, and the Electromagnetic Operating Environment (EMOE).

Modern conflict demonstrates how precision fires, pervasive autonomous systems, and ubiquitous sensing have created a transparent, highly lethal operating environment where the survivability of traditional platforms is severely tested. Within a contested EMOE, electromagnetic activities converge across offensive and defensive fires to simultaneously challenge and empower combat formations. As military theorists and analysts have observed, the kill chain has compressed from hours to mere seconds. Much like the post–Vietnam Army, which studied the hard-learned lessons of the 1973 Yom Kippur War to transform into the AirLand Battle force of the 1980s and 1990s, today's Army must transition a force forged in counterinsurgency into a formation engineered for the conditions of the modern battlefield.

Our formation bears an outsized responsibility for enabling the joint force to fight and dominate in Multi-Domain Operations. Information and intelligence no longer function as mere enablers; they constitute the modern warfighting architecture —the network is a weapons platform. Within this multi-domain fight, the 780th Military Intelligence Brigade develops, integrates, and delivers decisive cyberspace effects that tip the strategic balance.



Over the coming weeks, we will publish formal guidance detailing our three primary Lines of Effort (LOEs) – "**ROOT**". These efforts are designed to empower bottom-up initiative, providing a clear azimuth while enabling leaders to innovate rapidly. Underpinning these LOEs are our core command values: unwavering commitment to excellence,



care, ownership, and passion.

LOE 1: **Ready** the Force - centers on generating and sustaining our combat power. This line of effort goes beyond individual readiness to encompass the collective readiness of our crews, detachments, and specialized teams. We will ensure our entire formation—uniformed and civilian—is prepared to win, from individual work role training integrated collective exercises.

LOE 2: **Operationalize** and **Optimize** - focuses on maturing our forces and refining their design for the future fight. This effort involves not only optimizing our Cyber Mission Force (CMF) structures but also deliberately maturing our Army-Retained forces. A key objective of this LOE is to inform CYBERCOM 2.0 and improve our support to theater armies and the wider joint force.

LOE 3: **Transform** - guides how we adapt, improve, and codify the way we fight. Through initiatives like our Praetorian AI, Cyber Tradecraft, and Innovation (PACT-I) program, we will rapidly field emerging technologies, modernize our cyber infrastructure, and harness artificial intelligence. This transformation is fundamentally about enhancing our ability to deliver effects in and through cyberspace and to deliver decisive outcomes as part of the joint force in Large-Scale Combat Operations.

Driving this transformation requires intellectual agility and open professional discourse. I want to preserve and reinforce *The BYTE* as an indispensable vehicle for professional stewardship within our formation. True innovation rarely flows from the top down; it thrives when practitioners at every echelon actively challenge assumptions, dissect operational trends, and propose novel technical solutions. *The BYTE* serves as our dedicated forum to discuss, refine, and advance the cyber and intelligence profession. This journal further serves as our opportunity to tell the unique story of the Brigade's mission and operational advancements to the rest of the Army, the Joint Force, and the American public. I charge each of you—Soldiers, Department of the Army Civilians, and mission partners—to contribute your insights, publish thoughtful analysis, and lead the intellectual debate shaping the future of warfare.

I am deeply humbled and profoundly inspired to serve as your Ninth Commander. COL Boparai's leadership over the past two years leaves an enduring legacy of operational excellence, readiness, mutual respect, and a genuine "People First" command climate. I step into this role with complete confidence in the caliber, character, and dedication of this formation. As the Army's premier cyberspace operations brigade, your discipline and expertise in the shadows safeguard our national security and protect American lives every day.

Thank you for your dedication, your sacrifice, and your service. I look forward to serving alongside each of you.

Everywhere and Always...In the Fight!

Benjamin H. Klimkowski
COL, CY
Commanding



The Army Azimuth

By GEN Christopher C. LaNeve, 40th Vice Chief of Staff of the Army

SINCE 1775, THE UNITED STATES ARMY has defended our republic and carried the torch of liberty through suffering and sacrifice. From the frozen Delaware at Trenton to the bluffs of Normandy, the jungles of Guadalcanal, and the winter hills of Chosin, American Soldiers faced enemies in brutal conditions and held the line. They answered the Nation's call. One hundred and ninety campaign streamers fly from our Army flag, each testifying to the valor of our forebearers. Their legacy is ours to uphold.

Answering the Nation's Call

The Army serves the Nation. We preserve peace and security, support our national objectives, and overcome any force whose aggression imperils us. Our strategic direction is clear:

- *Defend the Homeland.* We secure our Nation's borders, protect the American people against attack, and respond to domestic crises — these are our most sacred duties. A secure Western Hemisphere is a prerequisite for joint power projection.
- *Warfighting.* America's Army applies violence decisively on battlefields marked by unrelenting speed, precision lethality, and persistent observation. We dominate from the outset to control escalation, prevent prolonged war and counter enemies who employ stand-off weapons, including unmanned systems and WMD.
- *Project Power On and From the Land.* The Army projects land power by generating combat credible formations, prepositioning capabilities where they matter most, and strengthening the capacity of our Allies and partners. The Army maintains units postured to respond immediately to crises and contingencies regionally and worldwide.

The Army is the Foundation of the Joint Force

The Army has aggressively pursued change to prepare for large scale combat operations. We shifted from brigade modularity to a force organized for multidomain operations at all echelons. We fielded long range precision fires that strike deep and sink ships at sea, evolved air defenses for skies saturated with unmanned systems, upgraded theater logistics, expanded terrestrial intelligence, and established new units integrating space, cyber, electronic warfare, and artificial intelligence into command and control.

The work of change continues. Today we emphasize the fundamentals of Soldiering, ensuring a strong grounding in warrior ethos, individual Soldier readiness, and small unit tactical skills. As the Army campaigns around the world, we turn our focus to operational readiness to achieve our central task: **To be ready to fight and win the battles and wars of the Nation.**

A ready Army is the foundation of the Joint Force, providing a range of capabilities that underpin joint operations and give our leaders immediate options. We employ four operational warfighting elements — convergence, strike, close battle, and endurance — to deliver joint all domain maneuver. We bind the regional land power networks of Allies and partners, offering distinct advantages for access and interoperability.

What Land Dominance Demands

U.S. Army forces must be prepared to overcome the most complex challenges our adversaries can impose and master an operational environment that looks fundamentally different from the battlefields of yesterday. To prepare for modern war, the Army will:

- *Embrace a Warrior Mindset.* We possess the grit to endure hardship and the courage to act honorably. Our Soldiers and Civilians uphold high standards and seek continuous development. Leaders at all echelons see Soldiers as the decisive advantage and prioritize training mission essential tasks.
- *Outpace our Adversaries*. We learn, innovate, and adapt faster by pairing our human ingenuity and judgment with advanced technologies like autonomy and artificial intelligence. Our professional military educational institutions teach the essence of warfighting, and our combat training centers validate readiness through crucibles designed to replicate the challenge of combat. Experience, reflection, and accountability propel our force to excellence.
- *Gain Positional Advantage.* We gain positional advantage through posture that comes in many forms: from forward basing to campaigning to stockpiling supplies. We continually reinforce forward areas, harden lines of communication, and exploit opportunities.

The next war will not look like our last. Yet there are timeless truths in war. The battlefield does not forgive weakness. Land combat in the modern era will demand every ounce of rigor, endurance, and courage we possess. Every shortcut in training and lapse in discipline will be paid for in blood.

This is the Army we must be: disciplined, lethal, and relentless — an Army that closes with and destroys the enemy, leaving no doubt about the will and power of the United States. As it has for more than 251 years, our Army will stand ready to fight, and win — whenever and wherever the Nation calls.

This We'll Defend!

Christopher C. LaNeve
40th Vice Chief of Staff
General, United States Army

LaNeve: Army Must Outpace Adversaries, Ensure Dominance

Association of the United States Army, published September 17, 2026

THE U.S. ARMY is the foundation of the joint force, and its leaders must work hard to outpace America's adversaries and ensure land dominance today and on future battlefields, Army Vice Chief of Staff Gen. Christopher LaNeve said.

In a Sept. 15 keynote speech on the opening day of the 2026 Maneuver Warfighter Conference at Fort Benning, Georgia, LaNeve, who also is acting Army chief of staff, called on leaders and soldiers in the audience to develop "a reservoir of mental fortitude" that will pull them through the toughest battles.

"Each of us has a moral obligation to our nation and the soldiers we serve to become the strongest, most lethal and most ready versions of ourselves," he said. He also urged leaders to "pursue excellence in our warfighting tasks and develop a reservoir of mental fortitude so we do not quit in the crucible of combat."

LaNeve reiterated the three warfighting requirements spelled out in "The Army Azimuth," his Aug. 19 letter to the force, a document that, he said, he and Sgt. Maj. of the Army Micheal Weimer wrote together.

"We intentionally chose every single word," LaNeve said, noting that he and Weimer "highlighted the three specific things the nation asks from the United States Army in our guiding document—defend the homeland, to fight and win wars and project power on and from the land."

First, to ensure land dominance, "everyone must embrace a warrior mindset," he said. "Our Army requires this of you, the close combat force. Full stop. You are in the business of closing the last 50 yards to the objective, destroying the enemy in the most grueling and unforgiving conditions, when asked."

Next, the Army must gain a positional advantage, which, beyond seizing key terrain, requires the force to think in terms of multidomain operations across a fully contested battle space. Lastly, to maintain land dominance, the Army must outpace its adversaries.

As 65% of the joint force, the Army is "not an option among several, it is the deciding force" because of what it brings to the fight, LaNeve said.

Army leaders and soldiers provide the joint force with detailed intelligence, sustainment, protection, connection between terrestrial-based sensors and space-based platforms and kinetic and non-kinetic fires "to destroy and degrade adversary capabilities," he said.

The Army also provides a "steady hand of cooperation and interoperability" with allies and partners, he said. "We campaign globally and, let's face it, most nations have an army, and their armies want to work with the best—us," LaNeve said.

"You in this room and the soldiers you represent require immense courage and mental toughness to persevere across the time and space of protracted conflict," LaNeve said told the audience. "There is simply no technology today that will replace what a soldier can do, and don't ever forget it. We, the United States Army, we do the hard thing, the intensely human thing, without hesitation, and close battle is what the U.S. Army provides to the joint force, and no other service can provide at scale." ■

U.S. ARMY

Intel Support to Cyber: *A quick look at the CMIG and other observations*

By CW4 (Retired) Michael Lewis, former 781st Military Intelligence Battalion (Cyber) Senior Technical Advisor

INTEL SUPPORT TO CYBER is no different than Intel support to Operations, kinetic or otherwise. As ADP 3-0 states, "The intelligence warfighting function is the related tasks and systems that facilitate understanding the enemy, terrain, weather, civil considerations, and other significant aspects of the operational environment." For intel support Cyber, the requirements to support Mission Elements (ME) may be different than what most intelligence personnel may be used to; however, the functions which support it are the same. I first opined this in a previous article of the BYTE (check it out here https://d34w7g4gy10iej.cloudfront.net/pubs/pdf_76851.pdf) which garnered interest from some of our senior leaders, and I was asked to visit the Cyber Military Intelligence Group (CMIG) to see if it changes my mind.

This is my assessment:

When I first arrived at the CMIG, I had little actual understanding of what the CMIG does, who they supported, and an assumption they only supported Defensive Cyber Operations (DCO). I spent a week with leaders from their SIGINT, GEOINT, HUMINT, and All-Source intelligence sections, which I found both familiar and, at the same time, different; particularly their requirements and processes.

I was surprised at their structure because they look, feel, and act as a Theater Military Intelligence Brigade (MIB-T), Analysis and Control Element (ACE). The ACE supports U.S. Army Cyber Command (ARCYBER) G2 (intelligence) requirements. The All-Source cell fuses intelligence from other intelligence disciplines to form a Common Operating Picture as well as respond to requests for information (RFI)s for support based on the priority of the request, the capability to respond, and the existing capacity to deliver in the requested time. Simple, right? The RFI process is the same primarily responsible for answering the commander's Priority Intelligence Requirements (PIR), which support both offensive and defensive cyber operations. As we sat down and discussed each individual section separately, I also noted the use of normal tradecraft, analytic integrity, and sourcing practices in line with ODNI Intelligence Community Directives (ICD) 203 and ICD 206. It became clear where operations varied from the traditional MIB-T were due to their individual customer requirements, which was expected. I also noted similar requirements and obstacles similar to those I experienced within the Cyber National Mission Force (CNMF) which I will discuss further below; however, before I do that, here are some of my initial observations *(Note: I will not go into too much detail here due to classification)*.

All-Source Fusion Cell:

They are the center-of-gravity for the ACE and create outstanding intelligence products, which inform the CMIG and ARCYBER commander's decision process. This is your operational, Phase 0, intelligence also called Intelligence Preparation of the Operational Environment (IPOE), or for us older folks, Intelligence Preparation of the Battlefield (IPB). I was shown multiple products of great quality and tradecraft which I would have appreciated during my time as the Deputy J2 of JTF-3, CNMF. If I had known about these target efforts at the time, I would have pushed for further organizational coordination which would have streamlined intel support for multiple organizations during times of urgency.

GEOINT:

They receive requirements from the Fusion cell supporting ARCYBER and CMIG specific requirements, utilized their discipline assist in Pattern of Life (POL) development, and provided great support to the target nomination process. Their use of GEOINT to support ACE efforts should be documented as lessons learned and sent to other intelligence organizations within U.S. Cyber Command (USCC), so they may utilize their GEOINT resources more efficiently.

SIGINT:

I had more assumptions about this section than most, due to my background; however, their requirements are completely different than the typical SIGINT element and this is directly due to their customer and their requirements which requires them to balance requirements not typical for the SIGINT community with the authorities they are given which forces them to accomplish the mission differently, and they are accomplishing it very well!

As stated above, it was clear most of their processes, products, obstacles, and complaints were close to those I experienced within the CNMF. This visit only cemented my opinion that Intel Support to Cyber is not any different than Intel Support to Operations in general. So, if it is all the same, why does everyone say it's harder? What are the common obstacles to providing this support? How do we streamline support? And what can we do as an organization to increase lethality?

Based on discussions with CMIG leaders and personal experiences from the CNMF, below are some of our thoughts:

Intel at echelon:

In discussion with CMIG leaders, one question which arose was "If intelligence

support to Cyber isn't new and ARCYBER is not unlike any other Theater Army, why doesn't ARCYBER have a traditional MIB-T? To my knowledge, the CMIG is the only element of its kind within CYBERCOM. That being said, I was recently informed of a new DIA Cyber Intelligence Center which may be producing a similar function, but I can't speak to it.

Within USCC, intelligence personnel on each Combat Support Team (CST)/ Combat Mission Team (CMT) are retained organically and included within their individual Mission Element (ME). Within CNMF, personnel on National Support Teams (NST)/National Mission Team (NMT) are broken apart and formed into separate Joint Mission Teams (JMTs) for each of the JTFs. Intelligence personnel at this echelon are focused on supporting their individual MEs and sometimes lack the support of higher level operational or strategic level analysis to support their targets. This could be from a lack of personnel, lack of requirements, or lack of time to provide support. Having a CMIG like element for each JFHQ-C/CNMF or employing the CMIG to provide support to the other JFHQ-C/CNMF elements would allow ME level intelligence personnel to focus on supporting tactical cyber operations with a larger understanding of the target operational space such as adversarial TTPs, potential larger scale risks and Centers-of-Gravity (COG).

Communication and Organization crosstalk:

There is a lack of communication across organizations both internal and external to CYBERCOM. I believe we are seeing a growing number of junior leaders within CYBERCOM, or one of its subordinate echelons, being retained in cyber elements for much longer than traditional Army tours which creates individuals having never been exposed to intelligence elements outside of USCC. This lends to an increasing culture of "the cyber way of doing things", potentially, with a limited understanding of intelligence resources available to the community. If leaders are uninformed on outside resources or external operations it can contribute to having organizations with similar or, potentially overlapping targets or priorities *(Note: Some of this is in the collection management role however it applies to staff as well)*.

Part of this could be fixed through educating leaders throughout the enterprise on intelligence capabilities across the theaters. Empowering junior cyber officers to be organizational leaders vs. only cyber operators with an insistence on movement to other mission scopes throughout their career could support more diverse exposure to operational and strategic level organizations.

Redundancy:

CYBERCOM, as an organization, is a confusing mix of entities tied to solid and dotted lines on a line-and-block chart and operating between administrative and organizational control. Having multiple echelons of commands in cyberspace with all conducting very similar missions has created the unintended side effects of scope creep. As this continues, some ME intelligence cells have simultaneously worked on intelligence products, for the same target, without knowing it. Generally, these types of products tend to be operationally focused products needed to provide additional target context.

Outside of USCC, each CCMD has an associated MIB-T which supports operational and potentially strategic lines of effort. In cyber, there is no MIB-T like element for each theater to provide that support. Like my note in the "intel at Echelon" paragraph, allowing the CMIG to support multiple elements, or creating a CMIG like element for each JFHQ-C/CNMF element, would help eliminate redundancy by providing further operational level product support.

Collection Management:

Collection management is central to intelligence community collaboration. From my experience the type of requirements primarily requested are organizational or informational versus technical, which can be critical to general target development. This includes getting approval for nomination to Joint Targeting Lists which also helps inform commander's decisions for prioritization. I believe some of the issues characterized above highlight how difficult it can be to utilize this program efficiently. This could be due to immature processes, uninformed leaders regarding outside unit capabilities, or external elements not responding to requirements. One course of actions would be to coordinate with the other MIB-Ts for support, they would be a great resource for operational level support. Another option would be to utilize the CMIG as an anchor point for the MEs to provide coordination. Both options could help provide further operational level intelligence and increased communication across the COCOMs.

These are just some of my observations and thoughts on how to make the organization better, however I do believe a DOTMLPF-P review would help identify better ways to streamline the organization as a whole. This visit also helped spark another thought process. Why not have a cyber force (like Army, Airforce, Marines, Navy Coast Guard and Space Force) providing support directly to the other COCOMs? Could this be another possibility which could solve some of the deficiencies identified? This could simplify communication lines, as well as priorities, in support of Theater level commands. Just something to think about.

Overall, my time visiting the CMIG was informative and enlightening. I appreciate the level of expertise and professionalism of their team. I would like to thank the Cyber Center of Excellence commander, MG Ryan M. Janovic; the former U.S. Army Intelligence and Security Command commander, MG (retired) Timothy D. Brown; and my command teams of the 780th MI BDE and 781st MI BN for the opportunity and support to visit the CMIG and provide some thoughts. Overall, I am just a lowly SIGINT WO and not the ultimate authority on intel support to cyber, but I hope this helps drive conversations throughout the community.

Thank you all and I hope this helps.


CYBER

Who Am I? Why Am I Here?

By SGT Jonathan Villarreal, C Co, 781st Military Intelligence Battalion (Cyber)

"WHO AM I? WHY AM I HERE?" is a quote from Medal of Honor recipient Vice Admiral James Stockdale spoken during the opening of the 1992 vice presidential debate. [1][2][3] Admiral Stockdale's delivery is perfect, it addresses that the audience doesn't know him or his background while also adding in the thought that maybe he didn't know either. Often times I fall back to this quote when thinking of my role as an All-Source Analyst (ASA) in the CNMF (Cyber National Mission Force). Most of the time our peers and some of our leaders don't exactly know what ASAs do, why we are here, and sometime we don't know either.

To answer the question of "Who am I?" you have to understand many things and most of them are not given up front as they should be or would be in a line unit. To give an example if you were a 35 series in a line unit they would break down the mission from the corps level down to your units METL or down to your individual task. Part of "who am I" is where I am slotted in the org chart and how does my mission nest into the mission of echelons above me. Being an ASA within the CNMF isn't strait forward as a line unit is or as clearly defined as it seems in the org chart in Attachment A. So, who am I, I am an All Source Analyst within a JTF (Joint Task Force), that is a part of the CNMF, that has a cyber focused mission set.

We have identified an obstacle. All Source Analyst, 35F, we are not cyber, we deal with maps, equipment specs, threat TTPs, unified land operations, we say things like LSCO and PMESII, we brief the weather when the SWO isn't there. That's what they teach us in AIT. Cyber to a 35F is one of the domains (Land, Sea, Air, Space, Cyber) and it certainly isn't the domain I had in mind when I enlisted or reenlisted. A new 35F in a line unit, in a TOC, is using all the INTs to create/maintain the COP (common operating picture) to brief during the CUB, and from that COP or intel make assessments and estimates as needed/directed. Nowhere in that foundational training is cyber involved, in fact training is done with a contested environment in mind so all of that work could and likely will be done in analog formats.

The solution, Cyber Threat Intelligence Analyst Course (CTIAC). A great course where intel meets cyber and the circle is made square for the issue explained above. The course is worth every minute and indeed answers questions that an ASA didn't even know they had (ASAs ask a lot of questions). In CTIAC we learn intel for cyber, we trade IPB for JIPOE, the battlefield becomes the operational environment, and zones (disruption, battle, support) become the 7 OSI layers. We gain all this knowledge on cyber and JIPOE and we come back to the CNMF but the next issue is "Why am I here."

I suppose I'm here to help the team but what is the team doing? The teams consist of the Soldier, Sailors, Airmen, Marines, Coasties, and civilians that are doing the groundwork on the target. The team knows that we can make slides and answer RFIs, it's a start. This misunderstanding of our role leads to RFIs that we cannot possibly answer unless they (the team) get their information reported. Example, an ASA would be hard pressed to produce a pattern of life analysis on a target that has one report produced about it. When enough of these interactions happen where an ASA appears ineffective or incapable our team starts to wonder why are we here and what exactly we do. Certainly, there is a bias from the team toward their INT causing them not give enough weight or thought into utilizing or requesting other INTs to answer gaps or confirm/deny the current analytical line.

So, why are we here? We aren't doing JIPOE everyday, we don't write white papers everyday, we aren't actively looking at the 7 layers everyday. Yes, we have the occasional baseball card or two and a company profile for a new target but the day to day role and function that we fill is reviewing, analyzing, requesting, briefing, and making sense of all the other INTs for our team. We are trading the maps for slides and emails, terrain and force objectives become target network and threat intent, and the BDA in now about networks and capabilities. We are here to provide context and intelligence from all the INTs relating to the threat and information environments to our teams.

References:

[1]https://mohmuseum.org/recipient/stockdale-james-bond

[2]https://www.war.gov/News/Feature-Stories/story/Article/2097870/medal-of-honor-monday-navy-vice-adm-james-stockdale/

[3]https://www.c-span.org/program/american-history-tv/vice-presidential-candidates-debate/133502/

Vanguard Food Drive









FORT GEORGE G. MEADE, Md – Soldiers and Civilians representing the 781st Military Intelligence Battalion (Cyber), Vanguard, donated more than 20,000 pounds of food and water to the Department of Veterans Affairs Community Resource and Referral Center Coordinator. The 781st MI BN ran the food drive over the past few months to help Veterans in the local area.

Facing Complexity: *Three Principles to Help Cyber Leaders Adapt their Organizations*

By MAJ Bryan Reasonover, Detachment Texas, 782d Military Intelligence Battalion (Cyber)

GENERAL CHRISTOPHER LANEVE, the Vice Chief of Staff of the Army, has challenged organizations to Outpace our Adversaries. [1]While the technological innovations that continue to congest today's battlefield have been heavily discussed, there has been very little professional discourse describing principles and actions for leaders when facing complex challenges that would allow for a marked advantage against our adversaries.

In the 782d MI BN (Cyber Legion) and Detachment Texas, the organizational leader characteristic that we value for complexity is adaptability. Army doctrine anchors the importance of adaptability with ADP 6-22 using the word adapt 69 times. [2]However, Army doctrine is not descriptive on how to develop adaptability or how to apply it. [3]An organizational leadership theory that can help leaders apply adaptability to outpace adversaries is "adaptive leadership" by Ronald Heifetz. [4]What follows below is an introduction to adaptive leadership and three principles to help leaders within the 780th Military Intelligence Brigade (Cyber) lead more effectively when facing complexity.

An Intro: Adaptive Leadership

Ronald Heifetz's adaptive leadership theory offers a way to lead in complex environments.[5] To help leaders characterize problems and determine what set of principles to use, adaptive leadership separates problems into two main types: technical or adaptive.[6]

Technical challenges fit the mold of traditional military problem-solving: well-defined with known solutions. In technical challenges, leaders themselves or authority figures with expert knowledge provide the solution. [7]Army Leaders are well practiced in solving well-defined analytical problems utilizing planning methodologies like the Military Decision-Making Process. [8]However, Army doctrine states that analytic decision-making is "not appropriate when forces must adapt to rapidly changing situations [emphasis added]." [9]A different set of principles is needed when facing adaptive problems.

Adaptive problems require a new way of doing things and cannot be solved with technical skills. [10]In adaptive problems, the solution is new and the bridge between the current conditions and the desired end-state cannot be connected utilizing current methods. [11]Furthermore, adaptive challenges require changing peoples' beliefs or ways of doing things. [12]Three leader principles to address adaptive problems are: regulate distress, maintain disciplined attention, and protect leadership voices from below.[13]

Regulate Distress to Learn Faster

Experimentation is critical to solving adaptive problems. [14]However, experimentation does not always end in success. Fear of failure and change creates distress within an organization. A leader's role in "regulating distress" is to maintain the proper amount of stress to generate change, but also to provide an environment of psychological safety for when experiments fail.[15] Good judgement comes from experience, but experience comes from poor judgement. [16]In Detachment Texas, when our units face uncertainty with complex problems, we have a saying – "make it an experiment!" Experimentation allows for creative and differing solutions to emerge, allowing leaders to better determine the way ahead to solve adaptive problems.

Maintain Disciplined Attention

Avoidance mechanisms are common when facing adaptive challenges. [17]Most of this is due to fear of loss of ways of doing things that once were valuable. The leader task is to identify what things in an organization are worth preserving and what things must be reduced for the organization not just survive, but thrive in the future. [18]Goleman provides six leadership styles to lead organizations: "visionary, coaching, affiliative, democratic, pacesetting, and commanding."[19] Regarding these styles, leaders that utilize greater than four of these styles have the most positive performance and organizational climates.[20] A broad range of leadership styles allows leaders to keep organizations focused on the uncomfortable tasks associate with change. In Detachment Texas, junior leaders ask "what leadership style should I use when facing complex problems?" The response is simple, but not easy: use the one that works.

Adaptive Characteristic	Adaptive Leadership Principle	DET TX Reinforcing Trait
Fear of failure	Regulate Distress	Make it an experiment
Avoidance of "big" issues	Maintain Disciplined Attention	Use the one that works
No known answer to problem	Protect Leader Voices from Below	What do you think?

(Table by author)

Protect Leadership Voices from Below

Adaptive problems cannot be solved with expert knowledge or current ways of doing things.[21] This type of challenge requires leaders to "relinquish" some control and disperse the responsibility of more individuals.[22] Protecting leadership voices is about making

for complex problems.

Adaptive leadership theory provides leaders with a framework to face the complex problems and obstacles associated with outpacing our adversaries on today's modern battlefields. Utilize the principles and reinforcing traits from this article to lead and drive adaptation within your own organizations. Get to work!

References:

[1]LaNeve, Christopher. The Army Azimuth. Accessed September 1, 2026. *https://www.army.mil/article/294744/the_army_azimuth.*

[2]Department of the Army. Army Leadership and the Profession (ADP 6-22). Washington DC: Department of the Army, 2019, Including Change 2, February 6, 2025. *https://armypubs.army.mil/ProductMaps/PubForm/Details.aspx?PUB_ID=1007609.*

[3]Barno, David and Nora Bensahel, Adaptation under Fire: How Militaries Change in Wartime, New York: Oxford University Press, 2020, p 250.

[4]Northouse, Peter. Leadership: theory and Practice, 9th Edition. Thousand Oaks, California: SAGE Publications, 2022, p 285.

[5]Northouse, p. 285.

[6]Northouse, p. 288.

[7]Heifetz, Ronald, Leadership Without Easy Answers. Cambridge: Harvard University Press, 1994, p 74.

[8]Command and General Staff College. "CGSC Circular 350-1". Author calculated Students spend 79% of classroom curriculum on planning methodologies (JPP/MDMP).

[9]Department of the Army, Mission Command: Command and Control of Army Forces (ADP 6-0). Washington DC: Department of the Army, 2026. *https://armypubs.army.mil/ProductMaps/PubForm/Details.aspx?PUB_ID=1033415, p. 24.*

[10]Heifetz, Ronald, "Adaptive Work." The Journal Kansas Leadership Center. Spring 2010. Accessed March 24, 2024. *https://www.hesston.edu/wp-content/uploads/2017/12/KLCAdaptiveWork.pdf, p. 75.*

[11]Heifetz, p. 73.

[12]Northouse, p. 290.

[13]Northouse, p. 293-298.

[14]Heifetz, p. 75.

[15]Northouse, p. 293.

[16]A common military adage. Paraphrased from a quote famously attributed to General of the Army Omar Bradley.

[17]Northouse, p. 292.

[18]Heifetz, p. 75.

[19]Goleman, Daniel. "Leadership that Gets Results." Harvard Business Review. March/April 2000, Volume 78, Issue 2, pp. 78-90.

[20]Goleman, p. 87; McCollum and Shea, "Adaptive leadership: The Leader's Advantage." InterAgency Journal. Vol.9, No. 1, 2018, p. 108.

[21]Heifetz, p. 73.

[22]Northouse, p. 298.

[23]Gemini Enterprise, "Animated solider sitting at a computer with paths leading through a cloud to a desired endstate." Image generated aby Google, August 24, 2026.



(Image generated by AI)[23]

Lethality in the Spectrum: *Transforming Expeditionary Electromagnetic Warfare for Future Combat*

By CPT Christopher Priestly, Detachment Hawaii, 782d Military Intelligence Battalion (Cyber)

IN THE ARMY AZIMUTH, GEN CHRISTOPHER C. LANEVE, the 40th Vice Chief of Staff of the Army, challenged the force to build the necessary "lethality and readiness" to "outpace our adversaries" in a highly contested operational environment (LaNeve, 2026). He emphasized that because "the battlefield does not forgive weakness," the speed of our adaptation and modernization is what determines our survival.[1] For today's expeditionary forces, that high ground is increasingly found within the electromagnetic spectrum (EMS).

For the Army's Electromagnetic Warfare (EW) community, maintaining lethality against peer adversaries requires a fundamental shift in how we conceptualize, train, and deploy Cyber Electromagnetic Activities (CEMA) assets. Drawing on broad tactical lessons from recent brigade level training rotations in highly restrictive, triple canopy jungle environments, this article explores how we can transition EW from a static, defensive enabler into an active, highly mobile "Multi-Functional" capability integrated at the tactical edge. To build a force capable of rapid, decisive multi-domain operations, we must focus our modernization efforts on three critical pillars.

Pillar 1: Shifting from Static Defense to Multi-Functional Reconnaissance

Historically, tactical EW assets have been employed as static, defensive enablers. During live fire exercises, EW platoons have often executed static surveys to generate targeting data. While doctrinally sound as a limited proof of concept, this static model is unsustainable against a peer adversary. It leaves teams highly vulnerable, restricts their mobility, and places immense sustainment burdens on dismounted operators. Furthermore, when EW teams are simply distributed across a battlespace without cohesive command and control, fragmented communications and a lack of physical mobility frequently reduce highly capable EW teams to passive early-warning nodes.

The future fight demands that EW move beyond passive monitoring. Modern combat lessons demonstrate the necessity of integrating low-signature EW teams directly into Multi-Domain Reconnaissance Teams (MDRTs) to execute a dynamic "sense, see, and strike" loop.

In this construct, EW operators act as proactive hunters. Operating beyond the Forward Line of Own Troops (FLOT), these teams use man-portable Terrestrial Layer Systems (TLS) to sense threat electromagnetic emissions and establish Lines of Bearing (LOBs). This immediate detection cues Small Unmanned Aerial Systems (sUAS) such as short-range reconnaissance (SRR), medium-range reconnaissance (MRR), or long-range reconnaissance (LRR) drones to fly out, locate, and see the target to achieve positive identification. Once validated, the team immediately strikes the high payoff target using organic precision assets through Low Altitude Stalking and Strike Ordnance (LASSO) or coordinated indirect fires.



To maximize this capability across the force, we must institutionalize the concept of Expeditionary EW Teams. When dense foliage or adverse weather grounds sUAS assets, the "sense-see-strike" model breaks. Expeditionary EW Teams in concept will resolve this by operating from highly mobile, low signature tactical utility vehicles equipped with onboard power generation. This will allow operators to quickly maneuver to optimal terrain, gain line of sight to enemy emitters, achieve movement-based triangulation, and rapidly displace before the adversary can execute counter fires after in-direct engagement.

Pillar 2: Technical vs. Tactical: Bridging the CEMA Integration Gap

Lethality is lost if the complex data our EW operators collect cannot be shared with maneuver commanders in real time. Across the force, we must address the critical technical to tactical integration gap. Tactical EW manpacks, which often operate on dedicated software-defined mesh networks, do not always natively integrate with the maneuver force's Common Operating Picture (COP) via the Android Tactical Assault Kit (ATAK) or MAVEN. This mismatch creates latency in sharing targetable data, forcing operators to manually relay coordinates. To streamline this process, the EW community must push for standard configurations that bridge civilian and military tactical architectures (CIV-TAK to MIL-TAK) to enable automated, instantaneous data transmission.

Furthermore, we must integrate CEMA planning directly into the Military Decision Making Process during the Mission Analysis phase. Historically, EW planning has occurred in an isolated technical silo, leaving maneuver commanders with a poor understanding of sensor placement, jamming ranges, and spectrum coordination.

CEMA planning must mirror the deliberate approach used by field artillery.

Just as an artillery officer templates firing positions, CEMA planners must template EW sensor locations phase-by-phase onto the COP, tailoring support to each battalion's platform ranges, power constraints, and target priorities. Utilizing modernized planning plugins within tactical mapping software allows planners to execute real-time line-of-sight (LoS) analysis, spectrum modeling, and power estimations. [2]As the Army continues to field advanced Electromagnetic Warfare Planning and Management Tools (EWPMT), our staffs must be prepared to use these systems to deliver a comprehensive, real-time picture of the electromagnetic operational environment to the commander.[3]

Pillar 3: Modernizing the EW Training Pipeline for Contested Environments

Building readiness for future combat requires an uncompromising, realistic training pipeline. In recent large-scale exercises, operators have often struggled with newly fielded Counter-sUAS (CUAS) systems. Brief blocks of instruction provided during initial staging are insufficient to prepare soldiers for dynamic, multi-directional aerial threats. However, when operators receive dedicated, hands-on coaching and tactical integration, their performance improves exponentially, enabling teams to successfully defeat over 90 percent of enemy drones during subsequent swarm engagements.

To prevent this training deficit in future conflicts, we must establish formal, unit-level CUAS Training and Certification Programs across our brigades. These programs must establish certified unit subject matter experts (SMEs) in every company who are proficient in system emplacement, battery lifecycle management, and antenna orientation. These SMEs can then train their organic teams, coordinate spectrum requests, and ensure that CUAS is treated as an integrated, baseline protective capability rather than an afterthought.

Additionally, we must shift our training focus to Counter-Electromagnetic Warfare (C-EW) operations. In a conflict against a peer adversary, our units will face sophisticated electromagnetic attack assets designed to jam our communications and spoof our GPS navigation. [4]We must train our operators to survive and operate in these degraded, communications-denied environments. Our training exercises must feature a robust, aggressive opposing force that actively jams our tactical networks. Operators must practice strict Emission Control (EMCON), utilize robust, redundant PACE plans (including high-frequency, TSM, and satellite beyond-line-of-sight systems), and deploy tactical deception (TAC-D) decoys to provoke enemy sensors into revealing their positions.

Act Now to Transform

The tactical lessons of recent jungle and expeditionary training rotations are clear: the electromagnetic spectrum is a domain that must be aggressively contested and won. As GEN LaNeve outlined in The Army Azimuth, our transformation must be continuous, ruthless, and rapid; we cannot afford to protect the status quo when our adversaries are aggressively adapting to match us. Our adversary is not waiting.

For the Army's EW community, transformation is an active, ongoing mission. By building expeditionary, multi-functional teams, integrating our sensor data directly into the tactical COP, and institutionalizing realistic, field-based C-EW and CUAS training, we will build the lethal, ready force required to fight, win, and dominate the future battlefield.

References:

[1]LaNeve, Christopher C. "The Army Azimuth." Official Homepage of the United States Army, *https://www.army.mil/article/294744/the_army_azimuth*.

[2]Nesaw, S. "Enabling Fires Modernization: How PEO IEW&S Supports the Fires Community." PEO IEW&S, 1 April 2025, *https://cpeisw.army.mil/2025/04/01/enabling-fires-modernization-how-peo-iews-supports-the-fires-community/*.

[3]PEO IEW&S. "PEO IEW&S Drives Rapid Prototyping." PEO IEW&S, 29 September 2025, *https://cpeisw.army.mil/2025/09/29/peo-iews-drives-rapid-prototyping/*.

[4]Watling, Jack, and Noah Sylvia. "Competitive Electronic Warfare in Modern Land Operations." Royal United Services Institute (RUSI), Occasional Paper, January 2025, *https://my.rusi.org/resource/competitive-electronic-warfare-in-modern-land-operations.html*.



Outpacing the Adversary: *How AI Enables Decision Dominance in Cyberspace*

By CPT Teisha Hardin, 102 CST Lead, 782d Military Intelligence Battalion (Cyber)

THE FORCE THAT TURNS TECHNOLOGY into combat power faster than its adversary will hold a significant advantage in future conflict. Offensive cyber operations sit at the forefront of this competition, where speed, adaptability, and decision dominance can determine operational outcomes. As the Army focuses on outpacing its adversaries, the Cyber Corps has an opportunity to pair the ingenuity and judgment of trained Cyber Soldiers with the speed and scale of artificial intelligence (AI). LTG Christopher L. Eubank, Commanding General, U.S., Army Cyber Command, recently emphasized this challenge, noting that defense of the Army's network is already "moving at machine speed" and that the force cannot rely solely on human personnel to operate at the speed required. Pairing human judgment with AI can accelerate the targeting cycle, improve decision-making, and enable Cyber forces to create and exploit opportunities before an adversary can adapt.

AI can accelerate the identification of opportunities, reduce the time required to develop capabilities, and enable leaders to make faster, more informed decisions. The objective is not technology for technology's sake, but the rapid conversion of innovation into combat power and operational advantage. Technology alone, however, will not create that advantage. The Cyber Corps must experiment with AI, train with it under realistic conditions, learn from those experiences, and continuously adapt how we operate.

Find, Fix, Finish, Exploit, Analyze, Disseminate (F3EAD) provides a useful framework for understanding how AI can accelerate the targeting cycle in offensive cyber operations. F3EAD relies on speed to convert information and operational effects into follow-on targeting opportunities. Each stage requires time, technical expertise, and coordination. AI offers an opportunity to compress that cycle and increase the speed at which Cyber forces can identify opportunities, create effects, exploit results, and generate follow-on actions.

During Find and Fix, AI can process large volumes of data, identify patterns and anomalies, and help operators recognize potential targets, vulnerabilities, and avenues of approach. These capabilities can reduce the time operators spend sorting through information and allow them to focus their expertise on information most relevant to the mission. Faster analysis can also help operators refine targets and identify opportunities before an adversary changes its posture.

During Finish, AI can support capability development, coding, technical analysis, and mission planning. AI-enabled tools can help operators work through complex problems faster and allow less-experienced operators to leverage institutional knowledge and proven techniques. AI does not eliminate the need for technical expertise. Instead, it can help Cyber Soldiers apply that expertise faster and at greater scale.

AI may provide an even greater advantage during Exploit and Analyze. Offensive cyber operations can generate significant amounts of data that operators must quickly process and understand. AI can help identify relevant information, correlate data, recognize patterns, and identify follow-on opportunities. During Disseminate, AI can rapidly synthesize that information for operators and leaders, generating new targeting opportunities that feed the next iteration of the F3EAD cycle.

The advantage does not come from accelerating a single stage. AI creates operational advantage when it compresses the entire cycle. Reducing the time between finding an opportunity, creating an effect, exploiting the results, and identifying the next opportunity allows Cyber forces to maintain tempo and act before an adversary can adapt. In an environment where both sides are constantly learning and adjusting, moving through this cycle faster allows Cyber forces to remain inside the adversary's decision cycle.

Achieving that advantage requires more than acquiring AI-enabled technology. ARCYBER is already operationalizing AI across its digital battlespace through a multi-year effort focused on AI-human teaming, accelerated analysis, and improved decision-making. These efforts demonstrate AI's potential, but the Cyber Corps cannot wait for conflict to determine how operators and AI should work together. Cyber Soldiers need opportunities to train with AI during individual training, collective exercises, mission rehearsals, and realistic cyber ranges. Training with these capabilities now allows operators to understand what AI can do, recognize where it can fail, and build the judgment required to employ it effectively in combat.

AI also creates challenges that traditional automation does not. An AI system can produce an answer quickly, but speed does not guarantee accuracy. In offensive cyber operations, acting on an inaccurate recommendation can create mission risk. Operators must understand when to trust an AI-generated recommendation, when to challenge it, and when human judgment must override it.

The Cyber Corps must therefore train Soldiers not simply to use AI, but to fight with AI while retaining human judgment. Technical proficiency remains essential. Operators who understand the underlying environment can better recognize inaccurate outputs, adversary manipulation, or recommendations that create unacceptable risk. Leaders must also understand these systems well enough to determine which decisions AI can accelerate and which require deliberate human review. Experience, reflection, and accountability must shape this process. Lessons from training and operations should inform how AI-enabled

capabilities are developed, employed, and improved, allowing the force to adapt faster with each iteration.

Our adversaries will not wait for us to perfect this approach. They will also use AI to analyze networks, identify vulnerabilities, develop capabilities, and support decision-making. Future cyber conflict will increasingly place human-machine teams against one another, with each side attempting to understand the environment, make decisions, and create effects faster than the other. The Cyber Corps must preserve the expertise of highly trained operators while using AI to amplify what they can accomplish. AI can reduce repetitive analysis, accelerate capability development, and provide leaders with relevant information faster. The operator will still provide mission context, evaluate risk, and apply judgment. AI does not replace the cyber operator; it enables that operator to act at a speed and scale that would otherwise prove difficult to achieve.

Outpacing our adversaries requires more than possessing advanced technology. It requires the ability to learn, innovate, train, and adapt faster than those we may face in combat. For the Cyber Corps, AI can help create that advantage by compressing the targeting cycle and allowing Cyber forces to identify, create, and exploit opportunities before an adversary can respond. Realizing that advantage requires experimentation and realistic training now, coupled with the technical proficiency, reflection, and accountability necessary to continuously improve how humans and machines operate together.

Decision dominance does not come from possessing the most data or the most advanced technology. We achieve it when we turn information into understanding, understanding into decisions, and decisions into effects faster than the adversary. Pairing the judgment and ingenuity of trained Cyber Soldiers with the speed and scale of AI can help the Cyber Corps do exactly that, allowing us to learn faster, adapt faster, and ultimately outpace our adversaries in future combat.

References:

[1]Wills, DeMarco, Staff Sgt. "Army Leaders Highlight AI, Human-Machine Teaming at TECHNET Augusta 2026." U.S. Army, August 25, 2026.

[2]Roman, Lindsay D. "Forging the Future: ARCYBER Integrates AI to Transform Cyberspace Operations." U.S. Army, July 31, 2025.



11th Cyber Warfare Battalion: *2026 Edition*

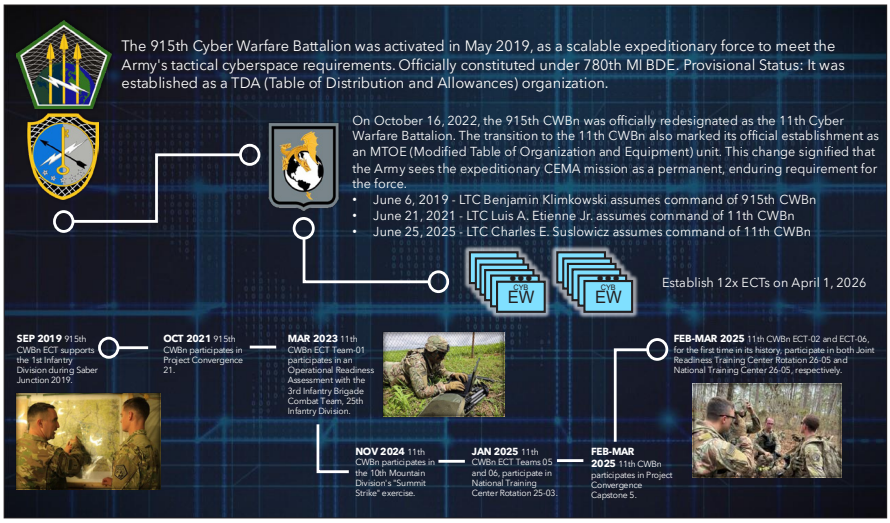
By CPT David Kim, 35A, CEMA Planner, 11th Cyber Warfare Battalion

THIS ARTICLE AIMS TO DISCUSS THE 11TH CYBER WARFARE BATTALION, at a high level, and the processes undertaken to achieve full maturation as set forth by its Concept of Employment (CONEMP). The article's scope is limited to the 11th CWBn's mission, structure and CONEMP (and its modernization efforts to fulfill those requirements), and training glidepath. Setting the scene, this article will briefly cover the unit's inception to its envisioned end state. The excerpt will then transition to the 11th CWBn's CONEMP and finally explain how the 11th CWBn is achieving said end states, as prescribed by the CONEMP, through training and validation exercises (VALEX), enabling the lethality of Expeditionary Cyber Electromagnetic Activities Team (ECT). These exercises (and support to operations) combined with Army Cyber Command (ARCYBER) modernization efforts inform the 11th CWBn's standard operating procedures (SOP). The lessons learned and observations will continue to transform the 11th CWBn into a more lethal force in the coming years.

Enter the 11th Cyber Warfare Battalion

The 11th CWBn is a unit unlike any other – its people, capabilities, and flexibility continue to adapt to modernization and Army needs. Many consider the cyberspace spectrum dominated by two fields. On the one hand, cyberspace operations – normally tasked to units such as US Cyber Command (USCC) Combat Mission Teams (CMT). On the other hand, the Electronic Warfare (EW) discipline occupies its own space, one that Forces Command (FORSCOM, now designated Western Hemisphere Command), traditionally subsumed, as seen in its Brigade Combat Teams (BCT) employing EW Soldiers and equipment from the Military Intelligence Companies (MICO) in the Forward Edge of the Battle Area (FEBA). The 11th CWBn leverages both worlds by fusing the more tactical EW subbranch with the technicalities of cyberspace operations to provide commanders with a single, versatile ECT, capable of achieving decisive effects across the full depth of the electromagnetic spectrum.

The Battalion is ready to deploy anywhere with *multi-faceted, tailored effect packages* to win in competition, crisis, or conflict. As the Army's only expeditionary CEMA force, 11th CWBn sets the standard for the Army in the Cyber domain. The mission of 11th CWBn: deploy Expeditionary Cyber Electromagnetic Activities Teams (ECTs) to gain tactical superiority in the Electromagnetic Spectrum, and Cyberspace to enable the delivery of Cyber Effects by the Remote Cyber Team (RCT) to increase the lethality of the Army across the conflict continuum.



Scene Setter - Command Relationships

To understand the 11th CWBn, we must understand who mans, trains, and equips the 11th CWBn. While the 11th CWBn is unique, it does share traits with many of its adjacent and higher headquarters units. These labeled "constraints" do not necessarily limit the Battalion but in fact the exact opposite, enabling the Battalion to leverage its relationships to conduct multi-faceted operations.

The OPCON/ADCON relationship described in *"Assessing the Army's Cyber Force Structure"* creates a fundamental challenge: Cyber Mission Force teams are operationally controlled (OPCON) by a joint headquarters but administratively controlled (ADCON) by their Army cyber brigade. This split often leads to conflicting priorities and a divided unity of effort between the team's operational tasks and its home unit's readiness requirements.

However, this structure provides a unique advantage. The direct OPCON relationship gives cyber teams intimate access to a joint commander's intent and operational needs, enabling highly tailored effects. Simultaneously, their ADCON connection to a specialized Army cyber brigade, the 780th Military Intelligence Brigade (Cyber), provides deep institutional support, advanced tools, and talent management. This duality places the units in a powerful position to translate arguably operational goals into precise tactical cyber actions, leveraging the best of both the joint operational environment and the Army's cyber enterprise.

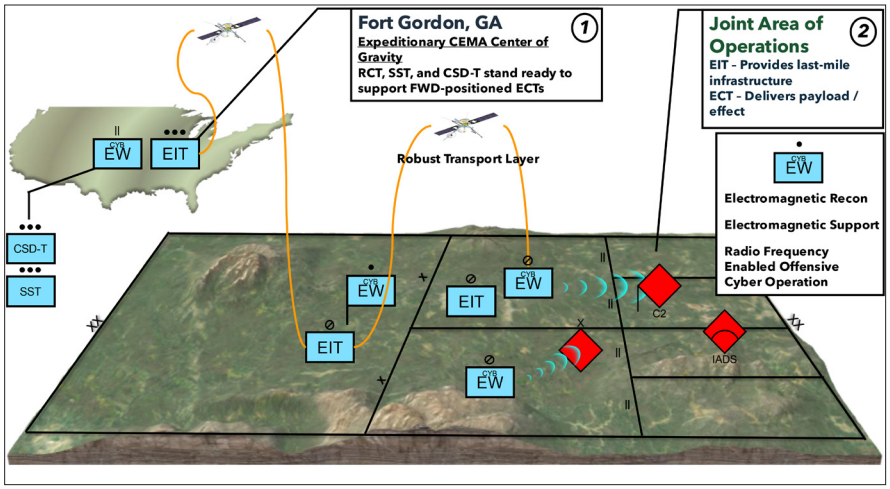
The Concept of Employment

11th CWBn's CONEMP is built upon a dual framework. This concept addresses

two fundamental and interconnected challenges: first, how to generate, prepare, and sustain a ready force for continuous global requirements; and second, how to structure and synchronize that force to execute its specialized, end-to-end mission process.

First, the 11th CWBn must operate under a highly iterative yet clearly delineated employment model. This overarching model that allows the Battalion to project forces at a moment's notice, support ongoing real-world requirements, but also generate the force with the knowledge, skills, and attributes to be lethal is the Sustainable Readiness Model (SRM). This framework is similar to the Special Operations' Joint Operations Readiness and Training System (JORTS) which provides balance between training, forecasted missions, and flexibility to response to with no-notice requirements. Of the twelve ECTs, four are on Red Cycle (recovery and individual to crew-level training), four are on Amber Cycle (crew and ECT validation), and four are on Green Cycle (presented to ARCYBER as deployable). An ECT's full SRM cycle is 18 months: six months in each cycle. At its core, the SRM enables the 11th CWBn to support all operations, train its force to assume mission, and offer predictability down to the lowest level Soldier on his or her team's glidepath to include recovery and training opportunities.

Second, to understand the CONEMP, we must examine how all 11th CWBn elements synergize to deliver effects that are inaccessible to a Combat Mission Team (CMT) and beyond the technical expertise of a standard EW formation. What makes the battalion unique is its "cradle-to-grave" process for generating non-kinetic effects. This integrated model begins with the Single-Source SIGINT Team (SST) identifying vulnerabilities, which are then passed to the Cyber Solutions Detachment – Tactical (CSD-T) to develop a custom capability. That capability is then delivered as either a conventional cyber effect by the Remote Cyber Team (RCT) or as a sophisticated EMS-enabled cyber effect, such as a target-specific protocol attack, by the ECT. This self-contained structure makes the 11th CWBn well-suited to fill its critical niche, providing Army Corps and ASCCs with a versatile weapon for the modern battlefield.



In Strides

The 11th CWBn is defining the future of the CMF by aligning its structure with strategic directives like CYBERCOM 2.0 and DoW's push for drone dominance while also formalizing its training. When it comes to The CYBERCOM 2.0 implementation plan, which outlines a deliberate evolution for the entire CMF, ongoing 11th CWBn efforts are already aligned with several key lines of effort aimed at building a more lethal and professional force. Among these are the directives to formally resource Mission Sets (LOE #5), to present forces with standardized tactical-level headquarters for effective command and control (LOE #6), and to implement a Unit Phasing model (LOE #7) sustainable rotations. While many units are navigating to this strategic shift, the 11th CWBn is already setting the standard. As a unit purpose-built for the specialized mission of bridging EW and cyberspace operations, it inherently embodies the spirit of LOE #5. The Battalion has already established a SRM with its ECRT and qualification courses, balancing mission, training, and reset periods in a mature cycle that directly aligns with LOE #7. Most critically, by structuring itself with an organic headquarters providing mission command to its ECT, the 11th CWBn has moved beyond the isolated "team model" and is pioneering the exact hierarchical and effective force structure envisioned by LOE #6. By doing so, the 11th CWBn is leading the way and providing a blueprint for the future of the Cyber Mission Force (CMF).

Additionally, the 11th CWBn is modernizing in other ways as well through aligning itself to the Department of War's (DoW) Drone Dominance Memorandum to further test the limits of sUAS integration with EMR, EMS, and RF-enabled OCO tools. These efforts weaponize platforms for non-kinetic effects, transforming drones into versatile assets for spectrum control and cyber operations and empowering ECTs with immediate, localized spectrum superiority.

11th CWBn also took initiative in the planned future implementation of the ECT Red Cycle Training (ERCT) and the ECT Table Qualification and Certification (ETQC) program represents a critical step forward for the 11th CWBn, establishing a comprehensive pipeline to man, train, and validate its specialized forces and paving the way for the battalion's future operational readiness. The ECT Red Cycle Training (ERCT) is the foundational, 13-week individual training pipeline that provides soldiers with the baseline skills required to join an ECT. This course covers everything from basic soldiering tasks like land navigation and weapons qualification to the technical job qualifications required for Cyber and EW roles. The primary outcome of ERCT is to produce a fully qualified soldier who has the fundamental expertise to begin focusing on collective operational requirements as part of a team.

Following ERCT, the ECT Table Qualification and Certification (ETQC) program provides a structured framework to

take these individuals and forge them into mission-ready teams. ETQC is a progressive, multi-stage process that uses qualification "tables" to validate team proficiency, starting with crew-level certifications and advancing through a series of increasingly complex Deployment Readiness Exercises (DREs) and culminating in a collective certification event. This structured path is critical because it creates a standardized and measurable process for building and validating ready and lethal ECTs, ensuring the Battalion can consistently meet its mission to provide deployable cyber forces for operational requirements.

Closing Words

The 11th CWBn's journey toward maturation, marked by its expansion to six ECTs (and soon 12 ECTs), showcases the unit's commitment to answering its calling. It is purpose-built to close the seam between EW and Cyberspace Operations, giving commanders an asset that can be a versatile enabler or a decisive surgical tool. This unique capability mandates an equally unique approach to readiness. 11th CWBn has embraced this challenge, developing a validation pipeline with the ECRT and ETQC that is as tailorable and demanding as the missions its teams will face, ensuring they remain the premier force of their kind.



RIFT: *Forging Readiness Before Qualification*

By 1SG Timothy Nicholas, Headquarters and Headquarters Company, 11th Cyber Warfare Battalion

A NEWLY ASSIGNED SOLDIER arrives at a cyber battalion eager to contribute. Within days, these Soldiers realize that becoming a fully qualified cyber professional takes years, not weeks, to develop. Limited training opportunities and finite resource constrain qualification pathways for U.S. Cyber Command and U.S. Army Cyber Command (ARCYBER) work roles. These constraints redefine the challenge from assigning Soldiers to a billet to developing Soldiers into combat-ready cyber professionals. The 11th Cyber Warfare Battalion (CWBn) answers the challenge through the Reception, Integration, Forge, and Transition (RIFT) process. 11th CWBn designed RIFT as a deliberate readiness framework with two objectives – talent management and standardized integration.

The Challenge

RIFT started as a commander and first sergeant initiative, focusing on improving accountability and readiness. Leadership quickly assessed that new Soldiers came from different backgrounds, ranging from initial entry training graduates to seasoned leaders from the Cyber Corps. Soldiers also in-processed with limited understanding of the opportunities available within ARCYBER. This friction led to lost time during one of the most critical periods of a Soldier's integration into the force. 11th CWBn did not accept this as an unavoidable challenge but chose to refine its approach to readiness.

RIFT evolved from rudimentary Battalion in-processing into a deliberate framework, establishing baseline assessments to measure aptitude and progression towards future work roles. RIFT accomplished this transition as the first phase of readiness generation, not a series of administrative tasks.

The Framework

RIFT has four phases – Reception, Integration, Forge, and Transition. Soldiers establish accountability during the **Reception** phase, completing administrative requirements necessary to enter the formation. Soldiers then enter the **Integration** phase, focusing on readiness through physical exercise, mandatory training, security requirements, and leadership engagements. Soldiers integrated into the 11th CWBn will be prepared for deliberate assessment and development.

11th CWBn forges cyber professionals through deliberate assessment and development in the **Forge** phase by using the Operator Development and Integration Evaluation (ODIE) alongside the Cyber Network Aptitude Battery (CNAB) to assess a Soldier's potential. Their current potential will lead them to one of four different pathways – Cyberspace Electromagnetic Operator, Electromagnetic Spectrum Operator, Cyberspace Operator, or Cyber Capabilities Developer.

Soldiers, upon entering a pathway, join the **Transition** phase. This phase prepares Soldiers for movement into their operational assignments with a clear way ahead for their current and desired pathway. This creates a common experience for all incoming Soldiers, receiving the same foundation, expectations, and opportunities while understanding their role within ARCYBER. Leaders gain greater visibility into Soldier potential, and Soldiers gain a clearer understanding of how their performance can influence future opportunities.

The Results

RIFT's influence extends beyond the 11th CWBn. The 11th CWBn works with the U.S. Army Cyber School, establishing recurring engagement to educate students and instructors on the significance of the ODIE and CNAB after graduation. These engagements placed emphasis on how these tools shape both the student's future and the Cyber Corp's future. Currently, 72 Soldiers have progressed through RIFT to include 54 Cyber Operations Specialists, eight Electromagnetic Warfare Specialists, and 10 from different military occupation specialties (MOSs).

Soldiers, prior to RIFT, arrived at the 11th CWBn with an average Operator Aptitude (OA) score of **260**. After engaging with the Cyber School, increased to nearly **450**. After completion of RIFT, Soldiers achieved an average OA of approximately **550**.

The most significant outcome, however, has been a change in mindset. Incoming Soldiers now arrive with a greater understanding of cyber pathways and the opportunities available within ARCYBER. Their motivation has increased, and they proactively inquire about potential opportunities, and they seek to understand how their individual performance influences their future development.

Assessments baseline an individual's understanding of aptitude and potential, enabling leaders to make more well-informed decisions and prepare Soldiers for future roles. Higher test scores, however, are not RIFT's greatest achievement. RIFT prides itself in the culture it fosters. Soldiers arrive at their companies better informed, more engaged in their development, and ready to assume ownership of their readiness prior to entering operations.

Leadership across every level of the 11th CWBn has contributed to RIFT's success. RIFT, originally a commander and first sergeant initiative, matured through the senior leadership and advocacy of the Battalion Command Sergeant Major. The deliberate management of Non-Commissioned Officers ensured both accountability and constant refinement. Their efforts transformed an initial concept into a repeatable framework for developing cyber talent and generating readiness.

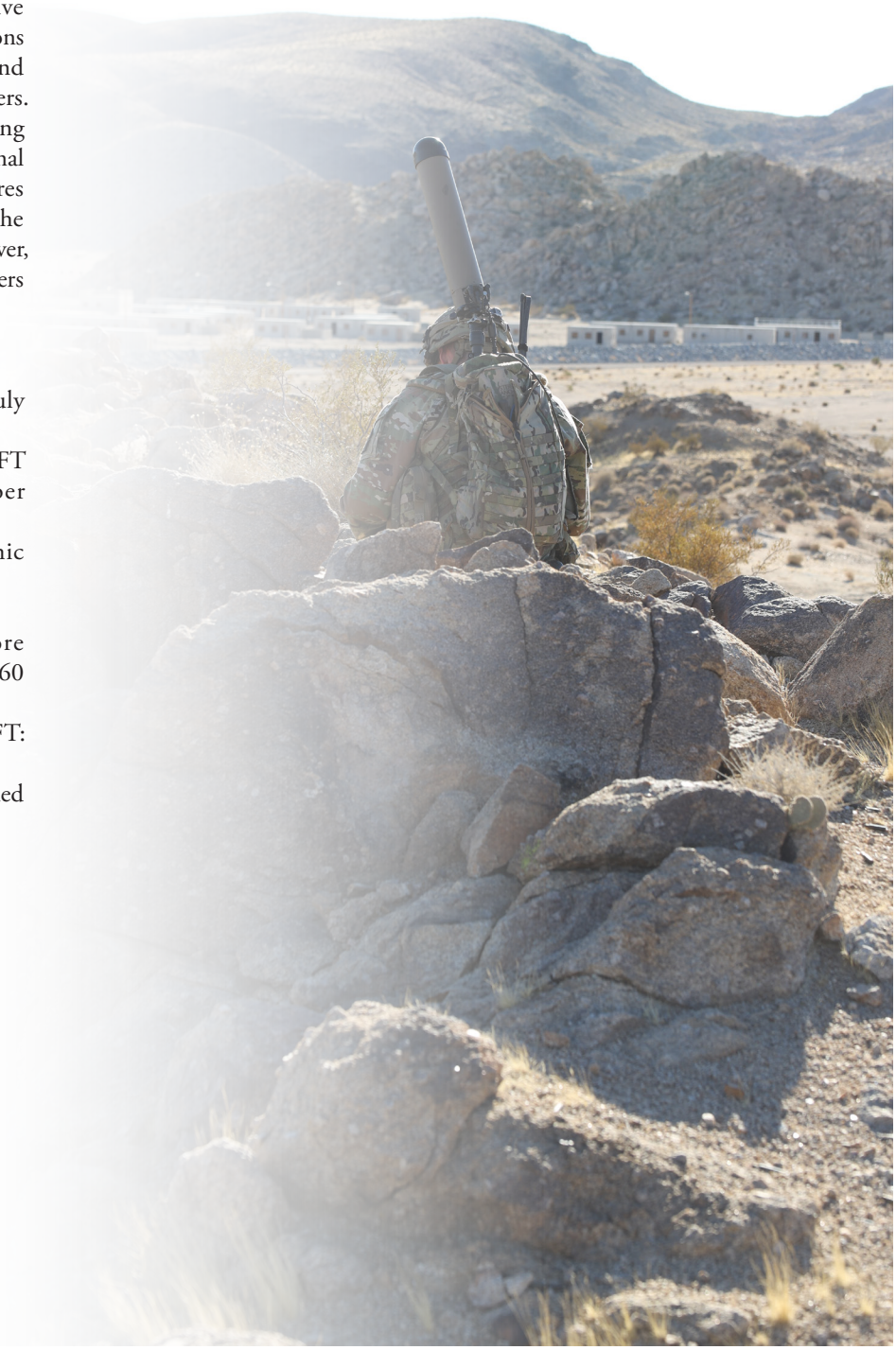
RIFT reinforces an enduring Army principle – talent management and readiness are inseparable. Early identification of strengths, establishment of expectations, and investment in development will generate meaningful combat power.

Shifting Readiness to the Left

RIFT's future centers on proactive force management. 11th CWBn envisions RIFT continuing to assess, develop, and qualify Soldiers early on in their careers. RIFT remains a dynamically changing framework. That establishes foundational work role requirements. These desires must be tempered by the needs of the Battalion. The desired end state, however, remains the same – mission-ready Soldiers post-transition.

Key Facts

- Timeframe: January 2026 to July 2026
- 72 Soldiers processed through RIFT
- 54 Soldiers from the Cyber Operations Specialist pipeline
- 8 Soldiers from the Electronic Warfare Specialist pipeline
- 10 Soldiers from other MOSs
- Average incoming OA score increased from approximately 260 to nearly 550
- Average OA score within RIFT: approximately 520
- Recurring engagements established with the Cyber School. ■











Applying Cyber Fires in the Right Place at the Right Time

By CPT Tate Bowers, Operations Support Element, 780th MI Brigade (Cyber)

The US military's concept of effective application of force is predicated on Combined Arms. For the Army to be lethal, it must put lethal force in the right place at the right time. Cyber is a key component of that in two aspects. It denies the enemy the ability to effectively deploy and coordinate onto target, and it nests with effective arraying of our own capabilities; acting as a force multiplier, as another form of fires. Modern militaries utilize multiple forms of combat power and mass them onto a single target to force the enemy into a situation where they cannot effectively maneuver and respond. The result is that enemy formations are broken up and friendly forces can take strategic objectives. The implied opposite situation, where fires are thrown independently, has the opposite effect. Without arrayed combat capabilities, the enemy is much more easily able to respond and counter our efforts, continuing their mission. Simply put, warfare from one domain does not achieve geostrategic goals by itself.

Combined Arms

Coordinating military capabilities is a fundamentally hard problem. Bringing the efforts of hundreds of thousands of people together for one moment in a key location is difficult. We have seen this repeatedly in Russia, where the institutional collapse of the Russian Air Force following the fall of the Soviet Union have led them to be unable to effectively gain air superiority against a nation effectively without an air force four years into the war[1]. They cannot exert air capabilities because getting the bombers, fighters, air defense, electronic warfare capabilities, artillery, and ground forces to work together requires training, exercises, and expertise well beyond what they had before the war began,[2] and any remnant died within months as they hollowed out their officer corps and training pipeline to limit the impact on the population.

As a result, Russia's cyber capabilities have had only so much impact in the conflict. They have not been able to turn cyberattacks that have crippled Ukrainian capabilities into exploitable events[3]. The Russian ground forces chose to move from maneuver combat towards borderline trench warfare, supported by significant artillery, mines, and EW, due to the collapse of their logistics chain and political demands. As a direct result, they cannot effectively take ground even when Ukraine is disrupted.

In this situation, the terrain is too deadly for infantry or even well-equipped brigades to penetrate the enemy's lines. The detection of massed attackers and effective counterfires by the defender means that operational situation is effectively stalemated. From the beginning of the conflict, when the Russian mechanized units fell apart because of lack of fuel, ground taking infantry, food, and ammo, to their air-raids, where groups of up to 12 strategic bombers lobbed bombs from the edge of their air defense bubble to today, where Ukraine is utilizing effective combinations of satellite imagery, Russian public data, and domestic long range drones to target the Russian economy[4,5], the front lines are too denied for maneuver warfare. That's not to imply that all future conflict will be that denied, it was a choice by Russia to anchor the conflict as they have and to misuse soldiers to try to attrite an enemy for years on end.

In this conflict, cyber did function as fires, as another form of artillery. Russia had fires superiority overall, but their geopolitical fixation on meatgrinders like Bakhmut meant that it did not affect the outcome. Where they massed fires, they could not mass sufficient forces to destroy the enemy. Where they massed forces, the area became too denied to mass vehicles, logistics, and fires[6]. They could not employ their capabilities effectively, fixating on winning messages at home rather than fighting the war[7]. A lot of people died. Pundits were entertained. The real outcome was borderline nothing for the greater war.

On the other hand, Ukraine effectively utilized their cyber, intelligence, and various other asymmetrical capabilities to severely degrade and disrupt Russian efforts. They defeated the Black Seas Fleet without a fleet in being. Russia fixated on the idea that they owned the sea, and Ukraine utilized low-cost drones combined with effective utilization of intelligence to destroy irreplaceable assets. They utilized Russia's refusal to take the war seriously and shipped drones right to the enemy's "secure" bases. They have productized and deployed long range drones en mass and have denied Russia the power of the Soviet inheritance.[8]

Cyber as Fires

That is how cyber is lethal. By identifying the enemy's key enablers and disrupting them at key moments, by destroying irreplaceable assets, by aligning geopolitical aims with actionable intelligence, and eliminating risks to the force. Cyber is fires in the same way that long ranged rocket artillery is fires. It has impacts up and down the chain but constantly firing doesn't necessarily produce the desired effects. Frequently, it causes the enemy to simply adapt and change their operational posture. From a business perspective, China destroying the servers, ransomware destroying the servers, or a hurricane destroying the servers are all about the same. What impacts the business is how quickly it can get back online and running. Throwing an exploit at an enemy server farm has a fixed business cost to recover. It does not impact operations unless it impacts a time

sensitive event.

The risks to the US military from cyber and electronic warfare are that it disrupts our actions at key moments. Coordinating the Air Force and Navy around Taiwan, while the National Security Agency and U.S. Cyber Command attack from back home will be met with similar attacks on the homeland. It would result in tens of thousands of dead Americans if our carrier groups were effectively targeted. China will also suffer significant causalities in an opposed amphibious landing as their first major military effort in decades. But for cyber to be lethal, and aligned to priorities, we need to focus on what cyber can effectively do. Even something as destructive as Stuxnet only delays. It needs to be aligned with geopolitical objectives and strategic aims. Even if a cyber operation managed to cripple the Chinese naval command and control system tomorrow, it would not change the fundamental geopolitical environment in the South China Sea. China, as an economic superpower, led by a visionary who sees the Chinese Communist Party as the successor of the Qing Dynasty[9], will continue to pursue their aims in the region. If the US is going to articulate cyber as fires, we need to treat it as fires and not aim for metrics that don't build towards something more relevant to geostrategic aims.

Russia has been waging a half-hearted strategic bombing campaign against Ukraine for years. They have had artillery superiority for years. They are supremely unlikely to "win", to achieve political goals that merit four years of grinding attritional warfare and result in Russia in a stronger geopolitical situation[10,11], given that they have lost far more blood and treasure than taking all of Ukraine will ever give back. And that happened while watching their geopolitical aims outside Ukraine collapse. Even if they won, they would end up with a constantly rebellious Ukrainian populace and a contiguous border with NATO, making the Soviet-destroying nightmare of the Afghani insurgency a comparatively far-off, low-impact threat. We cannot sell cyber based on temporary gains that the opposition can replace and operationally handle. For cyber to impact lethality, it needs to be applied as part of our concept of combined arms and nested with American and allied advantages, enabling the National Security Strategy. At present, the focus on a high op tempo and maximizing proxy metrics for lethality risks the opposite; simply revealing which servers our enemies need to have better backups for and hardening enemy systems against wartime attacks rather than enabling our strategic objectives.

References:

[1]*https://www.youtube.com/watch?v=-PCg-ba9tR* | The Ukraine Air War - The Russian campaign & does Ukraine need Western jets?

[2]*https://www.armyupress.army.mil/Journals/Military-Review/English-Edition-Archives/January-February-2025/Meeting-Expectations/.*

[3]*https://www.csis.org/analysis/cyber-operations-during-russo-ukrainian-war .*

[4]*https://www.wsj.com/world/russia/how-ukrainian-drone-strikes-are-pounding-russias-economy-a03652a7.*

[5]*https://www.wsj.com/world/europe/ukraine-bets-on-long-range-drones-as-it-seeks-a-battlefield-edge-90b83f30.*

[6]*https://understandingwar.org/research/russia-ukraine/the-kremlins-pyrrhic-victory-in-bakhmut/.*

[7]*https://www.youtube.com/watch?v=hx5mTslkUBs* | How Politics Destroys Armies: Politics, Factionalism & Russia's war in Ukraine.

[8]*https://understandingwar.org/research/russia-ukraine/gasoline-shortages-in-occupied-ukraine-show-the-synergy-of-ukraines-long-range-and-mid-range-strike-campaigns/.*

[9]*https://www.wsj.com/world/china/xi-jinpings-historians-cant-stop-rewriting-chinas-imperial-past-f59d6e2d.*

[10]*https://www.youtube.com/watch?v=94bqk8cB9iQ* | Russia's Grand Strategy and Ukraine - Is Putin's war already a strategic failure?.

[11]*https://www.gutenberg.org/files/1946/1946-h/1946-h.htm* | On War by General Carl von Clausewitz.



Adversary AI: How US Cyber Command is Adapting to the New Digital Battlefield

By PFC Ian Bortoluzzi, Operations Support Element, 780th MI Brigade (Cyber)

THE INTEGRATION OF ARTIFICIAL INTELLIGENCE into modern conflict has fundamentally shifted the center of gravity in cyberspace operations. What was once a domain dominated by human-driven intrusions and reactive patches has evolved into an active, automated war of algorithms. Artificial intelligence now acts as a definitive dual-edged technology. While it offers our forces unprecedented speed and visibility to secure an information advantage, it simultaneously grants foreign adversaries the capability to mount relentless, machine-speed attacks.

To achieve the lethality and readiness required for Multi-Domain Operations (MDO), the Army must answer a critical question: how do we dominate in the cyberspace domain, transform our forces, and stay laser-focused on innovating, training, and preparing?

Defining the Cyberspace Threat Landscape

The urgency of this transformation is driven by the rapidly evolving tactics of state-sponsored threat actors operating in the gray zone of competition. These adversaries leverage machine learning to bypass conventional defense-in-depth perimeters, transforming espionage and disruption into industrial-scale operations.

They deploy automated reconnaissance agents to perpetually probe global networks, mapping surface vulnerabilities at speeds no human team can match. Once an opening or a zero-day flaw is discovered, generative models rapidly assist in writing and weaponizing the code. Furthermore, these models have effectively eliminated language barriers, allowing threat actors to craft native-level spear-phishing campaigns and deploy sophisticated deepfakes of corporate executives and government officials to bypass multi-factor authentication norms.

Intelligence assessments also show foreign hackers covertly infiltrating open-source software development frameworks, injecting subtle backdoors into widely used code repositories to secure deep, persistent access to critical global infrastructure, threatening our strategic projection and operational freedom of action.

As Lt. Gen. Christopher Eubank, commanding general of U.S. Army Cyber Command, noted on the reality of this automated environment at TECHNET Augusta 2026, "The defense today of this network is moving at machine speed, the network you see today will not be the network you see in 90 days."

Modernizing Defensive Cyber Operations (DCO)

To counter these relentless threats and maintain domain dominance, U.S. Cyber Command and the broader defense enterprise are executing a profound strategic pivot to achieve operational-level overmatch. Moving past traditional bureaucracy, modern defense frameworks are transforming to focus on core pillars designed to maintain a decisive edge.

A primary focus is shifting away from manual incident response by deploying autonomous security layers capable of predicting, isolating, and neutralizing network anomalies in real time. This operational shift ensures that our defensive posture is as dynamic and unyielding as the automated attacks it seeks to defeat, preserving our command and control (C2) nodes in contested environments.

Equipping the Warfighter for the Cyber Domain

Simultaneously, the Army is laser-focused on accelerating operational timelines and training to meet these new demands. By utilizing dedicated research and development investments, targeted AI roadmaps, and rapid pilot initiatives housed within elite units like the Cyber National Mission Force, the military is compressing the sensor-to-shooter/sensor-to-effector loop from days down to seconds.

Bridging the gap between the military and Silicon Valley is equally vital to this preparation. Cyber Command leverages agile 90-day pilot cycles to rapidly test, validate, and scale commercial AI capabilities against real-world threats. By streamlining regulations and cutting through administrative friction, these initiatives foster fluid public-private partnerships, enabling federal agencies and critical infrastructure operators to deploy advanced security protocols without delay, reinforcing our defense support of civil authorities (DSCA).

Sustaining Readiness and Lethality

Ultimately, the digital frontier is no longer just a theater of espionage; it is an active, automated clash of intelligence systems where non-kinetic lethality is tested daily. As rival nations pour vast resources into weaponized code and autonomous operational tools, our lethality and readiness depend entirely on our cognitive speed. To maintain domain dominance against machine-speed cyber threats, the Army must rapidly integrate autonomous defenses, compress decision cycles, and leverage public-private innovation to out-automate the adversary. Lethality in cyberspace is now defined by cognitive and algorithmic speed.

National security and domain dominance hinge on the United States' ability to out-innovate, out-train, and out-automate the modern threat landscape, ensuring our forces are prepared for whatever the future of digital combat holds. ■


ADVERSARY AI
VS
USCYBERCOM
DEFENSE AI
ADAPTATION
RESILIENCE
ADAPTATION
DEFENSE AI
RESILIENCE
RESPONSE
BREACH
HACKING
COUNTER-
-MEASURES

Bandwidth, Power, and the Core Host

By CH Christopher Schafer, BDE Chaplain, 780th Military Intelligence Brigade (Cyber)

FROM THE CHAPLAIN'S DESK: Fellow Praetorians and Cyber Community colleagues, I am new to the cyber realm, but I am learning very quickly that everything has to do with connectivity. In quick observance one can note that if a terminal is disconnected from the host network, it has zero processing capability, cannot access shared resources, and therefore, within our domain, becomes virtually useless for the mission. Here is what I'm getting at; the even the most advanced, high-performance workstation is just dead metal and plastic if it is disconnected from the network or severed from its power source. That workstation is unable to generate mission throughput, defend networks, and/or execute mission. This is true for us too; and faith offers some incredible insight on this matter.

1. **Real "Throughout" requires connection**

In your daily work as Cyber Warriors, you are focused on productivity, defense, and high-tempo operations. Faith and spirituality reminds us that human effort alone has a hard limit. Just as a severed cable results in an immediate loss of signal, separating ourselves from our spiritual foundation leads to spiritual burnout, dry rot, and operational failure. For me as a Christian chaplain, I am reminded John 15:5 where Jesus uses analogy of him as a vine. The takeaway being that apart from the Vine, our spiritual throughput is exactly zero.

2. Watch out for "Connection Latency"

But even if you are connected, we all have experienced those moments when the system seems to just drag. For us it is easy to let the demands of the cyber mission crowd out our spiritual and psychological maintenance. When we stop praying, reading, or seeking fellowship, we introduce "latency" into our connection. We might still look like we are plugged in, but our internal battery is draining, and our resilience is drop-testing.

Faith and Spirituality gives us a central source of authority, power, truth, and operational direction in life. As individual operators, designed to process and execute output, we must remember that mission is entirely dependent on the connection. Maintaining an active, low-latency, unbroken connection to the core easily maximizes your capability to be highly productive. Let's be honest, you cannot run an enterprise-level mission on a disconnected terminal. If you want your life, your family, and your military career to bear lasting fruit, you must actively protect your connection to the Source of all power. If you would like to discuss more about making this connection or working on the connection latency, the 780th has incredible team of chaplains willing and ready to assist.





780th CYBER RETENTION

S T A Y P R A E T O R I A N S

780th Military Intelligence Brigade (Cyber) Change of Command Ceremony

By 780th Military Intelligence Brigade (Cyber) Public Affairs Office

FORT GEORGE G. MEADE, Md. – MG Rhett R. Cox, commanding general, U.S. Army Intelligence and Security Command (INSCOM), presided over a change of command ceremony whereby COL Candy Boparai, relinquished her command of the 780th Military Intelligence Brigade (Cyber), Praetorians, to COL Benjamin H. Klimkowski, on the McGlachlin Parade Field, July 14, 2026.

In a ceremony steeped in Army tradition, Soldiers, Family, and friends gathered to say farewell to the outgoing commander and her Family while also bidding a warm welcome to the incoming commander and his Family.

LTC Matthew D. Heinmiller, the brigade deputy commander, served as the commander of troops, and Command Sgt. Maj. Joseph Daniel, the brigade's senior enlisted leader and 'keeper of the colors' stood with the brigade color guard, along with the Soldiers representing the brigade's four major subordinate commands, the 781st Military Intelligence Battalion (Cyber); 782d MI Battalion (Cyber); 11th Cyber Warfare Battalion (CWB); and the Operations Support Element – a brigade with more than 1,500 personnel operating from four states (Georgia, Hawaii, Maryland and Texas) supporting multiple Army and joint commands.

The 780th MI Brigade (Cyber) was activated on October 1, 2011, as a Major Subordinate Command under the INSCOM, while serving under the operational control of U.S. Army Cyber Command (ARCYBER). The 780th is the only operational offensive cyberspace brigade in the U.S. Army, and generates, trains, and sustains the Army's offensive cyberspace operations teams and cyber warfare battalions to deliver effects in support of Army and joint requirements.

The brigade's strategic importance to the U.S. Army, U.S. Cyber Command (CYBERCOM), the Department of War, and our Nation was apparent by those who attended the ceremony, a veritable who's who in the cyber and intelligence community, including Mr. Brandon Pugh, the Principal Cyber Advisor to the Secretary of the Army; retired GEN Paul M. Nakasone, who served as the Commander of CYBERCOM and the Director of the National Security Agency (NSA); retired LTG William J. ("Joe") Hartman, a former 780th MI Brigade (CY) commander who led CYBERCOM/NSA; LTG Paul T. Stanton, Commander of the Department of War Cyber Defense Command and director of the Defense Information Systems Agency; LTG Christopher L. Eubank, Commanding General of ARCYBER; BG Matthew J. Lennox, Commanding General, Cyber National Mission Force (CNMF), also a former 780th MI Brigade (CY) commander; and an abundance of other senior Civilians, officers, warrant officers, and NCOs.

In his remarks, MG Cox referenced the historical importance of Fort Meade, from its establishment in 1917, as then Camp Meade, a training hub for Soldiers preparing for deployments during World War I and then renamed as Fort George G. Meade in 1929, processing more than 3.5 million Soldiers headed to World War II.

"But today, Fort Meade is our Nation's hub and center for its cyber and intelligence operations, and you're at the center of it… the 780th MI Brigade," said MG Cox.

He then mentioned, today, was a historic day, and a historic change of command for the 780th.

"As this team knows, probably better than most, we do not gather today in ordinary times. The cyber domain has been anything but quiet. We have witnessed a continuous unseen battle taking place every millisecond of every day," said Cox. "A relentless conflict that spans the globe. Networks have been tested, infrastructures been targeted, and the demand for resilient defense, precision cyber effects, and decision quality and intelligence has never been higher. Through it all the 780th has been in the fight on the front lines of the most contested domain in modern warfare."

MG Cox stated he couldn't be prouder of this brigade and what it has accomplished under the leadership of COL. Boparai.

"You took command during an era of unprecedented technological shift and adversarial aggression in cyberspace.



You led this brigade through it with skill, poise, and relentless drive," said Cox. "You build teams, you solve complex problems, you strengthen partnerships across the intelligence community, the interagency, the joint force, and with our allies. But I think, most importantly, you took care of your people while asking the best of them. The readiness of your formation increased exponentially."

His next message was for the Praetorian Soldiers and Civilians.

"Your commander changed today, but your mission did not. The world outside these gates remains hostile, remains uncertain, and our Nation depends on the work you do every day," said MG Cox. "Stay vigilant, stay professional, stay proud, keep adapting, keep delivering. Keep executing your missions and taking care of each other… God bless our Army, our Nation, our allies and partners. Everywhere and Always in the Fight…Vigilance Always, Always Out Front… This We'll Defend."

In her remarks, COL Boparai thanked the present commanding generals of INSCOM and ARCYBER, as well as MG Timothy D. Brown, who relinquished his command and retired on June 5, 2026; and LTG Maria B. Barrett, who relinquished her command and retired in December 2025, for entrusting her with the command, "being available, being approachable, and being great bosses."

She also wanted to, first, thank the people who made this day possible, including her superior officers and mentors, including GEN Nakasone, who mentored her since she was a captain and promoted her to lieutenant colonel and colonel; her peer groups, captain through colonel; her parents, who immigrated to the U.S.; and her immediate family – her son and her better half.

"So, the close friends I made along the way were the Family I got to choose. Not all of my friends could be here today, but it is not lost on me that some of the people sitting in the gazebo today are the same people who have, for decades, stood by me in hard times, and celebrated with me in good times, traveling for promotions and assumptions of command and graduation. Your Friendship means the world to me," said Boparai.

She also bragged on her unit. Her battalion command teams and staff; company command teams; the brigade staff; and of course, the best battle buddy ever, CSM Daniel.

And, then to her second point… her love for this brigade.

"I read an article recently about this GOAT debate, and it reframed the choice between Micheal Jordan or LeBron James as a choice between an athlete who enjoyed the best athletic peak, and one who has had the greatest period of sustained excellence that we will ever see," said Boparai. "And I thought about our brigade. The greatest period of sustained excellence."

"Teams built on time…check."

"Teams first on mission…check."

"Teams doing first Ops (operations)… check."

"Teams most trusted across the joint force…check."

"First off score across the joint force… check."

"The place the joint force comes to recruit talent…check."

"From the time this brigade stood up in 2011 until today, the 780th has projected a culture of excellence in our field, and that is because of each and every one of the Praetorians, past and present."

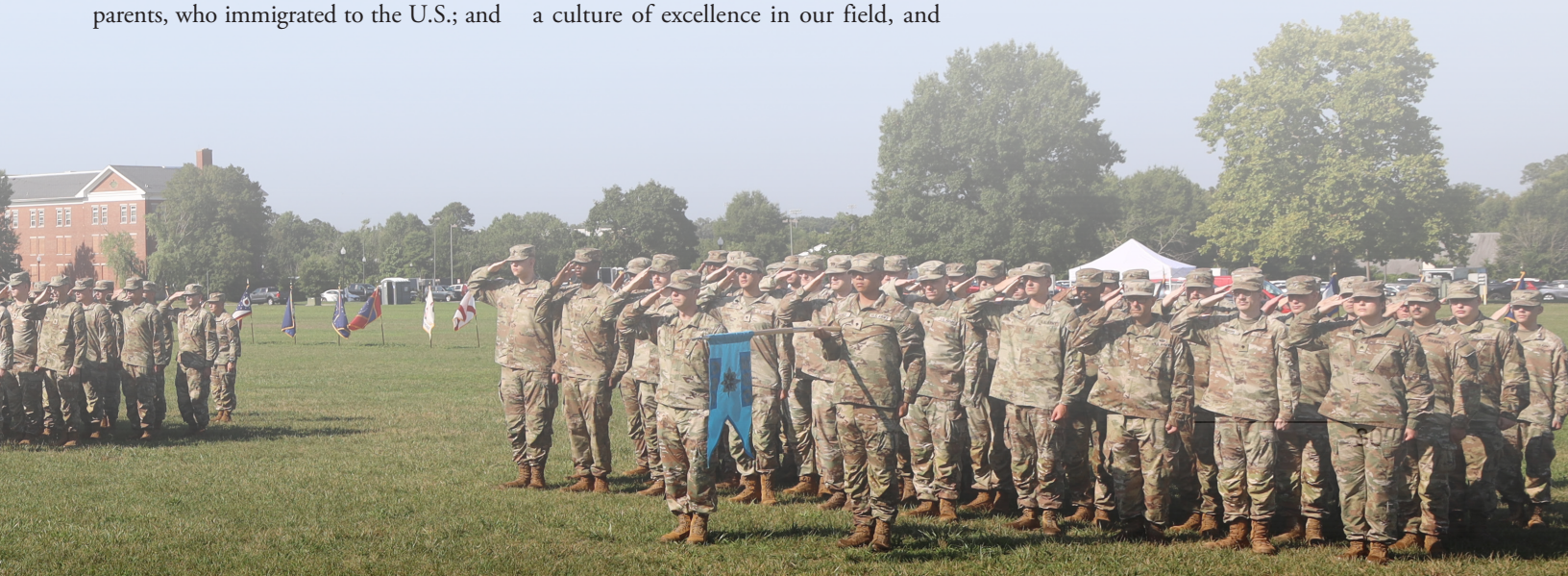
"Thank you for making the last two years deeply meaningful to me and just a sheer pleasure," stated Boparai. "Thank you for your service and commitment to each other and the mission."

COL Benjamin Klimkowski is no stranger to the 780th MI Brigade. Following his initial assignments with the 82d Airborne Division, he served at ARCYBER, taught computer science at West Point, and served in various positions in the U.S. Army Cyber Protection Brigade. He previously commanded the 11th CWBn, formerly known as the 915th Cyber Warfare Battalion.

"In keeping with our tradition, I will be completely committed to the highest standards of excellence and care," said Klimkowski. "And I will be completely committed to you as we relentlessly tackle the challenges of the future. Whatever our Nation calls us to do."

"Praetorian 6, logging in"
"Everywhere and Always…In the Fight"
"Vigilance Always"
"Attack and Defend…With Speed"

Ubique Et Semper In Pugna



Praetorian Change of Command











FORT GEORGE G. MEADE, Md. – MG Rhett R. Cox, commanding general, U.S. Army Intelligence and Security Command (INSCOM), presided over a change of command ceremony whereby COL Candy Boparai, relinquished her command of the 780th Military Intelligence Brigade (Cyber), Praetorians, to COL Benjamin H. Klimkowski, on the McGlachlin Parade Field, July 14, 2026.

AvengerCon X is a Wrap for 2026

By 780th Military Intelligence Brigade (Cyber) Public Affairs Office

LAUREL, Md. – AvengerCon X, the free cyber event specifically for personnel supporting the Department of War cyberspace operations, returned to Maryland for the Con's 10th anniversary at the Kossiakoff Center on the Johns Hopkins University Applied Physics Laboratory campus, June 30 and July 1, 2026.

AvengerCon is hosted by volunteers from the 780th Military Intelligence Brigade (Cyber), the Praetorians, to benefit the hackers of the U.S. Cyber Command and the DoW. The event features presentations, a hacker village, training workshops, and there was also an AMA-sanctioned FPV Drone Race.

CPT Ken McGaffey, a Praetorian cyberspace operations officer and the event lead for AvengerCon X, provided the opening remarks, followed by Dr. Joe Billingsley, Military Cyber Professionals Association (MCPA), who talked about the mission of the MCPA, and he emphasized it is not an industry association.

"(The mission) It's you. Those who are in the fight, today, and who have been in the past," said Billingsley.

McGaffey then introduced the AvengerCon X keynote speakers, Army MAJ Skyler Onken and CPT Andreas Kellas, both Praetorian alumni, who discussed the origins and growth of AvengerCon. Onken is an AvengerCon founder, currently serving as an Army Reservist, and co-founder of Twenty located in Arlington, Virginia. Kellas left the Army in 2021 and is a computer security researcher and PhD candidate at Columbia University.

"If you were in the 780th you were familiar with something called the Army Cyber Skills Challenge (*est. 2014*), which was ran by the warrant officers to really try to bring this warrior and cyber ethos together," said Onken. "This was about the best we had at the time for building what an identity was to be a cycle warrior. But simultaneous to that, there were debates as to whether or not you could be both technical and a leader…"

"So, in essence, the problem that we were looking at culturally was why do we have to dichotomize the process of being both a hacker and being a Soldier? Why was there a strange comparison, you can be technical, or you could be a leader, but you can't be both?" said Onken.

According to the AvengerCon founders, the goal was to define what it meant to be a cyber warrior. To create a culture that did not dichotomize these identities and allowed them to merge these two worlds together.

"If you look at what it means to be a hacker, it means that you are going to be curious, that you are going to be disruptive, that you're going to do things that are atypical or that are, maybe antithetical to the status quo. That culture is critical," said Onken "It's just what the nature of hacking was, is how we look at a system, how to find the loopholes or the unintended functionality within the system, and take advantage of it. And at kind of the surface level, that runs antithetical to what the military was pushing… And as we looked at it, we said, you know, if we don't actively try to merge these cultures together, the one will eat the other."

Kellas added that in a "good year" the brigade might send three of four Soldiers to Las Vegas to attend DEF CON – he did emphasize that there are other conferences and there are legitimate reasons why so few attend, i.e. cost and current operations; however, expecting those few to share the culture, the current creativity and disruption experiences presented and demonstrated at these public (and costly) cyber conferences, with others, was not realistic.

Leading off, the first guiding principle that really drove the creation of AvengerCon was this idea to bring the hacker culture to the Cyber Mission Force (CMF).

"***Why is the event called AvengerCon?***"

Because those initial founders, who developed the initial concept in a Johnny Rockets on the Las Vegas strip, where assigned to A Company, 781st Military Intelligence Battalion (Cyber)… *The Avengers.*

"The Soldiers who don't know the hacking culture – there's a number of us who were hackers before we joined the Army – and then there are those who joined the Army and want to be cyber awesome, they want to be a cyber Soldier," explained Onken. "They don't understand this outside culture. They don't even know that this world exists, or they only read about it online, and how do we bring this to them? We can't fly them out to Vegas every year. And we kind of (came up with this) idea, essentially, we should just throw our own DEF CON."

The second principle was of intellectual merit over rank. Since its inception, AvengerCon's uniform was "Hacker Casual." It emphasized that attendees were valued for their ideas, not their rank, and promoted open interaction among all participants. It was meant to instill an atmosphere where the most junior Soldier (Sailor, Marine or Airman) would feel comfortable contributing.

Principle three was AvengerCon is for the Soldiers. Their focus then and now, is not on the keynote speaker, the sponsor, the organizer, or the general officer – it was an opportunity to the Soldier to give their first talk.

"Annually, this is something we've returned back to, especially in our AARs (after action reports). Did we achieve success in terms of keeping the focus on Soldiers," said Kellas.

It would have been very easy for the AvengerCon organizers to invite a general officer; however, Onken stated the keynote speaker selection was very intentional.

"If our in-state was to merge these worlds, so that every Soldier could benefit from essentially a wider community and a way of thinking about cyber warfare and cyber operations, that was kind of moralistic as to what the technology, what the environment entailed. We realized we needed to bring in different people," said Onken. "Year one was

Eugene Spafford, and year two was Bruce Potter, and then year three was Chris Eagle… and then year four Daniel Cuthbert… that was all very, very intentional in the way that we did that." See AvengerCon History at *https://avengercon.com/history* for the full list.

The topic of the mid-day panel, in honor of AvengerCon's tenth anniversary, was the "History of the 780th Military Intelligence Brigade (Cyber)." The 780th is the Army's only offensive cyberspace operations brigade and will celebrate its 15th anniversary on December 1, 2026.

Although there might be some curious about the highlighted panel topic, those who heard the panelists or know of our history (notwithstanding as short as it is) know the significant impact of our people, past and present, on the origins, growth and maturity of the military cyber enterprise and ensuring our nation's security.

The panel members, introduced by COL Candy Boparai, the commander of the 780th MI BDE (CY) commander, included COL (Retired) Benjamin Sangster; CW5 John O'Reilly; CW5 (Ret.) James Richards; CSM Ronald Krause; and Mr. Chad Dickerson.

"We continue to evolve, as Skyler (Onken) spoke about, 'who would have thought of seeing drone racing at AvengerCon' and yet this is where we are. So, who knows what the future will bring, but events like this truly help us at the 780th and in the Cyber Mission Force to broaden our horizons and just continue to grow," said Bopari. "Sklyer and Andreas spoke about this culture of curiosity, and just always wanting to learn, and I agree with (them), that this is really emblematic of that culture."

The panel moderator, LTC Robert Frost, brigade S3 (Operations), asked the panelists questions ranging from the unit's biggest challenges to solving problems and challenges.

"I think, for me, the thing we've done the best, looking back over my entire time in the brigade and the CMF, is that we have normalized our independence," said Richards. "So, when I started in the CMF, it was everything was ad hoc. Everything was the first time. You could see people writing awards for the end of tour, and everything was, did this for the first time, did that for the first time. And I also wondered how many of those things were the only time we did that, because we were experimenting and trying to figure it out."

Frost left the audience with two thoughts on behalf of the group.

"First, about a decade ago, then Colonel (Jennifer) Buckner said something that when they were building this whole ship, they were 50 percent confident that they got 25 percent of it right," said Frost. "To echo something the sergeant major said to those of you who are still in, you have the opportunity to change it, and then something else that stuck with me over time… I personally wish if I had been more thoughtful back in the day, you know, maybe we would have solved problems earlier. Your senior leaders enjoy feedback. They seek it out from you who are at the tip of the sphere. Help us shape the next ten years of both AvengerCon and the Brigade."

Much like other hacker conferences there were presentations throughout the day in the main auditorium, as well as in the adjoining APL classrooms.

A huge shout out to all our second day presenters from the Praetorian Brigade to our sister unit, the 91st Cyber Brigade, U.S. Army National Guard; from the CMF, to academia, and industry. The topics ranged from 'Smartphone OPSEC Risk: Mobile Apps that Target U.S. Service Members and their Families' to 'AI and Social Engineering in Offensive and Defensive Cyber Operations', from 'npm install && pwned: A Field Guide to the npm Malware Landscape' to 'Becoming and Exploit Developer in the Age of AI.'

The results of the first AvengerCon X FPV Drone Race, , organized by CPT Ryan Johnson, 780th MI BDE (CY), who is also a member of the Army Drone Team, was in fourth place, Ensign Joey Mentel U.S. Naval Academy, FPV Pilot name: JoeM7; third place Ensign Caden Warren, USNA, FPV Pilot name: BanquetFPV; second Place, CPT Sam Fox, 780th MI BDE (CY), FPV Pilot name: UnfilteredFPV; and first place, WO1 Jerimiah Katen, 780th MI BDE (CY) FPV Pilot name: iCrashFPV.

Much gratitude to our partners – the Johns Hopkins Applied Physics Laboratory, the Army Cyber Institute at West Point, and the Military Cyber Professionals Association – as well as our sponsors and exhibitors.

We hope to see all our in-person and virtual attendees back for AvengerCon XI in the spring of 2027; and we will hope to see you at HammerCon V, hosted by our MCPA partners, hosted here at the Kossiakoff Center, on the JHUAPL campus, September 24, 2026.

Ubique Et Semper In Pugna

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

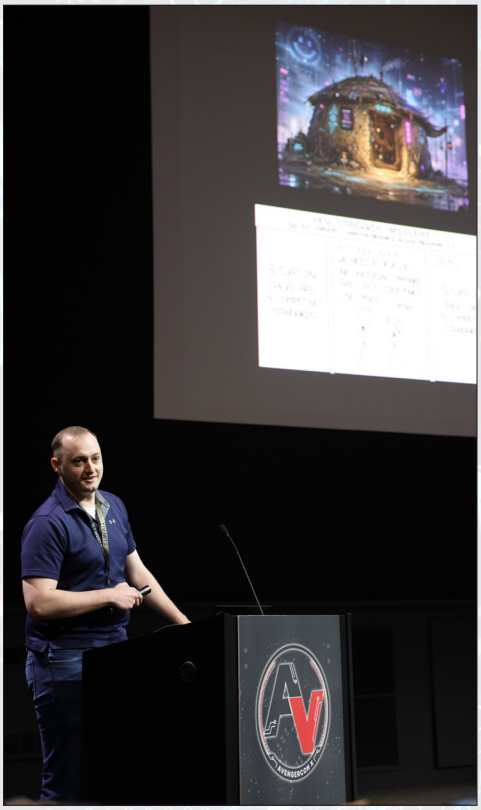



JUNE 30 - JULY 1
AVENGERCON.ORG
Offensive Cyberspace Operations
"Everywhere and Always In The Fight!"
780th MI BDE

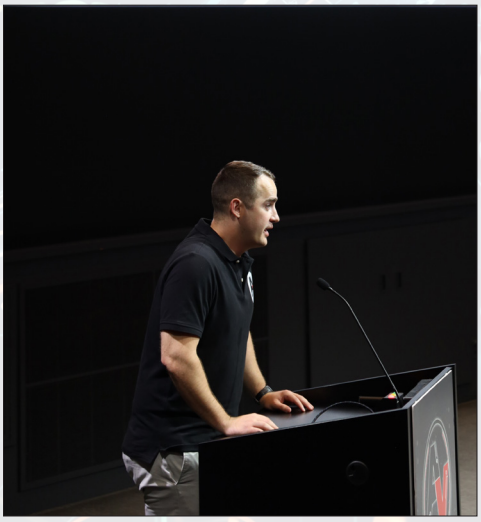

The Local Chapter Welcomes You!
milcyber.org
RECOGNITION • EVENTS • PUBLICATIONS
CYBER




// avengercon-x
780th MI BDE History Panel
COL Candy Boparai
COL(R) Benjamin Sangster
CW5 John O'Reilly
CSM Ronald Krause
Mr. Chad Dickerson
Hosted by LTC Robert Frost




Process injection primitives on Linux




Hacker or Soldier?
Technical or Leader?
Why not both?

Some Retirement Remarks from CW4 Michael Lewis, former Vanguard Senior Technical Advisor

By CW4 (Retired) Michael Lewis, 781st Military Intelligence Battalion (Cyber)

"FRIENDS AND FAMILY of the 780th Military Intelligence Brigade (Cyber) and extended enterprise. If you didn't know, I have decided to retire after 23 years of service. While my career has been a long one, it's flown by. It has been a bittersweet time for me, but I know I'm ready to start this new chapter. I couldn't get around and see everyone as I transitioned out of the unit, but I wish you all good luck and God speed with everything you do. Since I have access to a platform to spread some knowledge, I would like to impart some advice as I go:

1. Don't stay in the same place for too long. I know it's nice to have stability and really get to know your mission. Whatever that may be. However, from my experience this is a quick way to get pigeonholed into one mindset and limit your flexibility and your chances for opportunities to look at problems in a new way.
2. Somewhat connected to #1, Seek out opportunities for something different. You know you'll hear people say, go for the hard jobs. I tend to agree. Do something new, try new concepts, try and figure out ways to make it work. It keeps things fresh, but it also really does round you out as a person.
3. To my Enlisted community, you really are the workhorse of the Army, the "Backbone of the Army"! Doing what needs to be done: training, planning, executing, day-to-day taking care of Soldiers. The one thing the Army is good at producing is leaders. Remember, that is what all of you are. No matter what it is you do, always take pride in your work and do the best job you can. Be confident you did the best job you could and that you didn't "half-A—it". If you pay attention to the details, it will ensure you are successful and it will lead to more success in the future.
4. To my Officer Corp, you are the leaders, commanders, decision makers. You all provide the purpose direction and guidance which sets the stage for how operations are conducted and the overall mission execution. Remember to be humble and empower the other cohorts. Seek advice, delegate responsibility and hold accountable those within your sphere of influence. This little bit will help you be successful throughout your career. I can appreciate the level of stress that comes with being an officer, especially in this day and age. Keep your head up, build your team and don't be afraid to ask for support. This will take you further than you think.
5. To my fellow Warrant officers, the technical experts… (By the way, for my Officers that want to stay technical, the Warrant Officer path is the way to go, just saying.) As Warrants, you must be the subject matter experts. Take the time to hone your craft. But you can't stay so focused that you do nothing else. As Warrants, we cannot only be the expert in the craft, but we need to understand how our craft fits into the bigger picture. We are technical experts but also leaders, mentors, teachers, and advisors. As you progress through your career, you must look at how the Army works and be able to work with Officers to properly advise them along the way. I built my career trying to figure out how to get to "yes". Sometime the answer is no, but that is after all efforts are made to support. Then the "no" comes with reasons why and potential other possibilities. Build your network. The ability to have a network and build relationships will help you get the job done. Remember to reach out, ask questions, and use the Warrant network. I guarantee someone else may have faced a similar situation.

Again, I appreciate all of you for guidance, friendship and support along the way. The one thing I appreciate most about the military is the People. This organization brings people from all backgrounds, lifestyles, races, colors and creeds from around the world AND we make this work. It is truly beautiful and I'm so grateful that you all have become a part of my story. If there is anything I can do to help any of you, just let me know. Thank you all so much!

Chief Lewis, signing off.

Cyber Battalion's Senior Technical Advisor Retires after 23 years of Army Service





FORT GEORGE G. MEADE, Md. – Chief Warrant Officer 4 (CW4) Chad Mastbergen, Command Chief Warrant Officer, 780th Military Intelligence (MI) Brigade (Cyber), presided over a retirement ceremony for CW4 Michael Lewis, senior technical advisor for the 781st MI Battalion (Cyber), in recognition of his 23 years of faithful service at the NSA Cryptologic Museum, July 16.
780th Military Intelligence Brigade (Cyber), Praetorian Change of Command Ceremony!

HHD (Herculians), Operations Support Element, 780th MI Brigade (Cyber) Change of Command ceremony







FORT GEORGE G. MEADE, Md. - Major John E. Rollinson, Commander of the Operations Support Element (OSE), 780th Military Intelligence Brigade (Cyber), hosted a change of command ceremony whereby Captain Christina L. Hunter relinquished her command of the battalion's Headquarters and Headquarters Detachment, Herculians, to Captain Alexandre Dang at the McGill Training Center Ballroom, June 23.

OSE elements build, sustain, and provide teams to support the Cyber Mission Force's offensive cyberspace operations, develop operational capabilities, and enable utilization of cyberspace operations infrastructure. ■

HHC, 780th MI Brigade (Cyber), Hastati, Change of Responsibility Ceremony





FORT GEORGE G. MEADE, Md. - CPT Amanda K. RoperBrooks, commander, Headquarters and Headquarters Company (HHC), 780th Military Intelligence Brigade (Cyber), hosted a change of responsibility ceremony whereby 1SG William S. Kinsley, the outgoing senior enlisted leader and keeper of the colors, relinquished his responsibility as company first sergeant to 1SG Nevada C. Henricksen at the Fort Meade Post Theater, June 29.

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





FORT GEORGE G. MEADE, Md.. - LTC Daniel S. Hawthorne, Commander of the 781st Military Intelligence Battalion (Cyber), 780th MI Brigade (Cyber), hosted a change of command ceremony whereby CPT Daniel V. Alvarado relinquished his command of B Company, 781st MI BN, to CPT Ethan A. McInturff at the McGill Training Center Ballroom, September 9. ■

Brigade Suicide Prevention Hike









At the very core of effective suicide prevention lies a dedicated commitment to ***foster deep, mutually enriching human connections that are proven to combat harmful behaviors and prevent suicide****. Organized in partnership with the 780th Military Intelligence Brigade (Cyber) and 781st MI Battalion (Cyber) Unit Ministry Teams, this hike is intended for us to join arm-in-arm in solidarity, demonstrating that no one carries their burdens alone.*

Within our community, our Unit Ministry Teams stand on the front lines of this mission, providing compassionate pastoral care, absolute confidentiality, and unwavering support to service members and their families navigating distress or isolation. Genuine social belonging does not simply alleviate loneliness, but it actively dismantles the alienation that often precedes self-harm, creating a shared path where individuals can voice their struggles without fear or judgment. By stepping forward together and weaving resilient bonds across our formations, this hike transforms fellowship and human connection into an active, visible, and life-saving intervention.

– SSG Brittany N. Reyes, Religious Affairs NCO, 780th MI BDE

Praetorians organize and participate in Royal Danish Air Force March



























FORT GEORGE G. MEADE, Md. - The 780th Military Intelligence Brigade (Cyber), Praetorians, organized and conducted the Royal Danish Air Force March for Fort Meade tenant units to earn the RDAFM ribbon to promote physical fitness and foster esprit de corps, August 28.

SFC Derek Tien and SSG Riley Draves, 780th MI BDE, organized and completed the 20 kilometer route, which required participants to complete the RDAFM / Danish Flyver event with a 10 kilogram ruck. There were over 500 participants from throughout the installation, representing units from all the services.

The brigade supported the event by coordinating with garrison staff, route and support personnel, including road guards, water points, a trail vehicle, and CLS personnel with aid bags. ■

NEXT QUARTER'S BYTE IS a look back on where we've been and where we're going – the Brigade's 15th Anniversary. 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 October 15, 2026. Final articles are due October 31.

