THE PROFESSIONAL BULLETIN OF THE U.S. ARMY SIGNAL REGIMENT

ARMY COMMUNICATOR

CONNECTING OUR PAST • POWERING OUR PRESENT • SECURING OUR FUTURE

CELEBRATING

166TH BIRTHDAY OF THE U.S. ARMY SIGNAL CORPS

JUNE 21, 1860 - JUNE 21, 2026

1860

FROM TELEGRAPH LINES TO GLOBAL NETWORKS, OUR LEGACY BEGAN MORE THAN A CENTURY AND A HALF AGO.

COMMEMORATING 250TH ANNIVERSARY OF OUR NATION

JULY 4, 2026

250 YEARS OF LIBERTY. 166 YEARS OF COMMUNICATION. ONE NATION DEFENDED.

Approved for public release; distribution is unlimited. | Headquarters, Department of the Army. | PB 11-26-3 **Summer 2026**

In This Edition:

U.S. Army Signal Regiment Leadership

43rd Chief of Signal and U.S. Army Signal School Commandant,

Col. Julia M. Donley

26th Regimental Command Sergeant Major,
Command Sgt. Maj. Lisa M. Gandy

8th Regimental Chief Warrant Officer,
Chief Warrant Officer 5 Willie L. Newkirk

Army Communicator

Editor-in-Chief,
Laura Levering

The Army Communicator is published as a command information e-publication for the men and women of the United States Army Signal Corps under the provisions of AR 360-1. Opinions expressed herein do not necessarily reflect the views of Office, Chief of Signal, the U.S. Army or the Department of Defense.

Send articles, photos, graphics, and story ideas for the Army Communicator to the editor-in-chief at laura.m.levering.civ@army.mil.

On the Cover:
The U.S. Army Signal Corps celebrates 166 years of "getting the message through." From Albert J. Myer's pioneering wig-wag system and Civil War telegraph lines to today's global communications networks, Signaleers have remained essential to defending the nation. This commemorative cover also honors the 250th anniversary of the United States on July 4, 2026 – 250 years of liberty, 166 years of communication, one nation defended. (*Cover design and photo illustration by Tài Doick, U.S. Army Signal School. Some imagery incorporates AI-generated elements that were digitally enhanced, composited, and refined by the creator)*

43rd Chief of Signal Signing Off the Net, Honored to Have Served

Being your Chief of Signal has been the pinnacle of my career. I feel absolutely honored to have served this Regiment as its chief for the last two years and to have served alongside all of you for the last 26 years. In this role, I've had the privilege to honor the past, nurture the present and prepare for the future. The Army Communicator has played a key role for decades in each of those areas: articles remembering the past, documenting the present and thinking to what we will be in the future.

Reflecting on the Past

I've asked many of you to be a part of the conversation by ***writing*** and ***publishing*** in this great journal of ours. And I haven't asked you to do anything I wouldn't do. I was first published in the Army Communicator, Fall 2005 edition. Recently returned from my second deployment in support of Operation Iraqi Freedom, I recorded 121st Signal Battalion's achievements as one of the largest Mobile Subscriber Equipment (MSE) networks ever built: eight companies; 60 nodes; 1,027 Soldiers; passing an average of 125 gigabytes per day in support of 15,000 customers. Twenty years later, a historian reached out to ask if he could use that article as a primary source in his book about the greatest signal battalion in the Army, "**Danger's Voice**!"

You will find me again in the Summer 2007 Army Communicator edition, this time detailing 67th Signal Battalion's deployment and role as the strategic backbone for Multinational Forces Iraq. And I have been honored to kick off each edition with some thoughts on where the Regiment has been headed for the last two years. When we take time out of our ever-busy schedules to think, write, and document, we never know what sort of impact those efforts will have. I don't know if any of you will be contacted 20 or 30 years from now by a historian asking permission to use your words, but I do know that everything you write down fills in just a bit more of the exceptional and elaborate 166-year network of our great Regiment.

Being present

The absolute best part of my job is talking to brand new Signaleers – whether they be Soldiers in training, newly branched cadets, or just arrived warrant officers in Warrant Officer Basic Course (WOBC). Anyone who derides the newest generation has never sat in an information technology specialist (25B) Advanced Individual Training (AIT) class or spoken at an Officer Candidate School graduation. I've had the honor of commissioning nearly 200 cadets, many of them with shiny new crossed flags on their collars. Some of them I've spoken to as they considered which branch was best for them, been there when they raised their right hands, welcomed them to Fort Gordon, and then pinned on their Regimental crests at the end of that 10-mile ruck tradition. I can tell you that they are smart, dedicated, and eager to do all they can to make the Signal Corps proud.

As the Army rebalances, we will be filling the newly returned division signal battalions with this new generation. The most recently graduated Signal Basic Officer Leader Course had someone headed to nine of the 10 divisions, and as each AIT and WOBC class wraps up and ships out, they will be going all over the world. Wherever you find the U.S. Army, you will find a Signaleer there – doing the hard work of providing command and control with the latest technology, as we have done since the Civil War.

Looking forward

Technology will change, but the mission doesn't, and the Signal Corps isn't going anywhere. For 26 years, I've heard a rumor that technology will make the Regiment obsolete. The truth is that technology only gets more complicated and places a heavier burden on the Signaleer. The telegraph may have replaced flags and

torches, but it still needed the Hello Girls to operate it. There is a 26B (data systems engineer) at the heart of 4th Infantry Division's Next Generation Command and Control (NGC2) efforts. There is a 25U (signal operations support specialist) making software-defined radio networks easy to use. There is a 25A (signal officer) ready to help their commander figure out how to install Mobile Application Management Intune on their personal device. There is a 255N (Network Operations Warrant Officer) going on their third sleepless night trying to configure Seeker. There is a 25Z (Visual Information Operations Chief) working overtime putting together a training plan to make it all work. These people, ***all of you, Signaleers***, are a part of the ***future*** of our Army.

There has not been a single technological advancement in 166 years without a signal Soldier there to help figure it out. Looking back reminds us that tomorrow's challenges are solvable. We have taken flight. We have explored the poles. We launched into space. Take heart, for we have been ever watchful for our country and will continue to be so for as long as our Army goes rolling along.

Pro Patria Vigilans!
Watchful for the Country!

Col. Julia M. Donley,
43rd Chief of Signal and U.S. Army Signal School Commandant

Col. Julia M. Donley places the U.S. Army Signal Corps branch insignia on a signal officer-inductee's uniform during a regimental induction/pinning ceremony for Signal Basic Officer Leader Course, Class 003-26, on May 28, 2026. (Photo by Laura Levering, U.S. Army Signal School)

The Enduring Signaleer: Understanding the 'Why' and 'How'

In modern multi-domain operations, mission success hinges on our Signaleers' ability to establish, maintain, and defend resilient communication networks. We can no longer rely on contracted engineers and field service representatives to build, maintain and troubleshoot our networks – or to train our Soldiers. Building and maintaining resilient networks require that Signaleers be the absolute master of their equipment, possessing the deep technical knowledge required to keep the network alive when isolated.

The contemporary operational environment is characterized by sophisticated electronic warfare and persistent cyber threats. Our adversaries understand that disrupting command and control (C2) is the fastest way to paralyze a force. Therefore, troubleshooting is a critical warfighting skill.

An enduring Signaleer ***must*** understand the ***why*** and the ***how*** behind the network, moving beyond rote memorization of standard operating procedures. When a network is under a cyber attack or facing kinetic threats, Signaleers must rapidly:

- **Diagnose and Isolate**: Act as forward-deployed cyber defenders to identify anomalies and isolate compromised nodes before it impacts across the network.
- **Execute the PACE Plan**: Seamlessly transition between Primary, Alternate, Contingency, and Emergency communication plans. This means effortlessly jumping between multi-orbit satellite communications, high-frequency radios, and line-of-sight systems while utilizing diverse waveforms and encryption standards.
- **Restore C2**: Apply ingenuity and fundamental signal theory to physically and logically rebuild degraded networks on the fly.

A resilient network is forged in training, and commanders bear the responsibility for driving this standard. Leaders must require tough, realistic training environments that replicate the friction of multi-domain combat. Establishing networks in sterile, interference-free motor pools fails to prepare Soldiers for the reality of war. Commanders must enforce training that actively stresses the system and the Soldier:

- **Degraded Environments**: Introduce simulated jamming, spoofing, and severed fiber lines into field training exercises to force Signaleers to troubleshoot under pressure and execute their PACE plans.
- **Signature Management**: Evaluate units on their ability to minimize electromagnetic signatures, seamlessly employ Low Probability of Intercept/Low Probability of Detection waveforms, and maintain rapid mobility to evade simulated enemy kinetic strikes.
- **Cyber Hardening Drills**: Routinely test strict adherence to cryptographic standards, rapid patching protocols, and zero-trust principles at the tactical edge.

Ultimately, the most critical component of a resilient network is the Signaleers themselves. Equipment will fail, signals will get disrupted, and weather will degrade transmissions. The enduring Signaleer is defined by their adaptability, elite technical and tactical proficiency, discipline, and relentless drive to restore the link. Technology provides the tools, but it is the tough, realistic training repeated over time (*Reps and Sets!*) that is demanded by leaders – and the resulting troubleshooting mastery of the Soldiers – that ensures the commander's voice always reaches the frontline.

Signal Proud! Signal Strong!

Command Sgt. Maj. Lisa M. Gandy,
26th Regimental Command Sergeant Major

The Enduring Signaleer: Building a Resilient Network for the Future Fight

As the U.S. Army transitions its strategic focus toward large-scale combat operations (LSCO) and multi-domain operations, the tactical communications network transcends its historical role as a mere enabler. It is now a primary warfighting system and a critical operational center of gravity. When communications fail, operational momentum stalls, situational awareness degrades, and the commander's decision cycle is critically lengthened.

While modern technology, including software-defined architectures and advanced satellite transport, delivers unprecedented capabilities, these tools alone do not engineer resilience. The true foundation of network survivability is the technically proficient, tactically disciplined Soldier. It is the enduring Signaleer who ultimately transforms technological capability into decisive combat power.

The operational assumptions that underpinned two decades of counterinsurgency operations are no longer valid. Near-peer adversaries now possess sophisticated electromagnetic warfare (EW) and cyber capabilities deliberately designed to locate, exploit, and destroy friendly communications. In this threat landscape, network survivability is equally as critical as data throughput.

To survive the modern targeting cycle, mastery of electromagnetic spectrum operations (EMSO) is mandatory across all echelons. Every electromagnetic emission presents a potential signature, making traditional, static command posts highly vulnerable. The enduring Signaleer must minimize these signatures, seamlessly employ Low Probability of Intercept and Low Probability of Detection (LPI/LPD) waveforms, and maintain rapid mobility to evade enemy kinetic strikes.

For true network resilience, the Army must move away from an over-reliance on civilian field service representatives (FSRs) and contractor support. In a highly contested logistics environment characterized by denied airspace and disrupted supply lines, civilian support may not reach the tactical edge.

Signal warrant officers must serve as the catalyst for cultivating organic technical curiosity within tactical formations. Junior operators and noncommissioned officers must be trained to independently understand the intricacies of dynamic routing protocols, radio frequency propagation, cyberspace defense, and cybersecurity fundamentals. Formations equipped with this intrinsic knowledge can rapidly troubleshoot hardware and software failures, adapt to changing environmental conditions, and independently restore mission capability under extreme operational pressure.

The concept of Primary, Alternate, Contingency, and Emergency (PACE) communications is foundational to signal doctrine. However, PACE plans are functionally useless if they exist only as conceptual diagrams on briefing slides. True operational resilience requires routine training under purposefully degraded conditions, transforming theoretical alternate communication pathways into an instinctive, unit-level reflex.

Building the Enduring Signal Regiment

The operational environment and the equipment fielded to combat formations will constantly evolve. Artificial intelligence, cloud computing, and proliferated low Earth orbit (pLEO) constellations will reshape the tactical edge. Yet, amidst these advancements, people remain the decisive factor in network survivability.

Signal leaders must demand unyielding technical excellence and enforce rigorous training standards. By fostering a culture of organic troubleshooting and tactical discipline, the Army ensures its communications infrastructure can withstand enemy disruption.

The enduring Signaleer remains the ultimate safeguard, ensuring our networks remain resilient and capable of providing secure, rapid communications to the warfighter, anywhere, at any time.

Chief Warrant Officer 5 Willie L. Newkirk,
8th Regimental Chief Warrant Officer

Ch-ch-ch-ch-changes …

Laura M. Levering
Editor, U.S. Army Signal School

"Changes." The song (by David Bowie for you young folks, circa 1970, I believe?) popped in my head as I began writing this editorial. As long as I have been editor of the Army Communicator (since April 2022), each edition has included a suggested theme or topic for Signaleers to consider writing about. When the Harding Project launched in September of 2023, I anticipated changes would ensue – and the Army Communicator would be impacted – but at the time, I had no idea to what extent. The scope of changes, from both my purview and that of others directly involved, was unforeseen. At its core, the Harding Project aims to ***revitalize professional military discourse*** through writing. It sounds simple enough – but is it?

Just as the Harding Project has changed the way we operate here at the branch journal, the Harding Project itself has also changed drastically. One of the project's primary components – the Harding Fellow – began as an appointed (temporary) assignment. It has since evolved into a competitive, three-year broadening program in which selectees earn a fully funded master's degree in journalism and mass communications from the University of Kansas (please read more about it here). It is an exciting opportunity intended to improve (directly impact) all aspects of the fellow's respective branch journal, working with the civilian editor as a "team." Several journals have a Harding Fellow in place, and the program is proving to be a success with the Fellow being a significant asset. Having said that, we (Army Communicator) are not projected to receive a Fellow until 2028 at the earliest. Subsequently, the effect has forced changes to the way I operate here.

One of the most visible changes you can anticipate is the quantity and quality of content published in future editions of the Army Communicator. We must strive for ***quality***; not quantity. We are transitioning away from quarterly themes to focus more on what you – the Signaleer – have to share of value to the force – whether it be for Signaleers or Army at large. Do not limit yourself. Explore Line of Departure online and download the app. Not only does it house the Army Communicator, but it will give you a better idea of what Soldiers across the force are doing and the types of articles being featured (and sought by senior leadership).

Speaking of Line of Departure … Do not wait until the upcoming edition's deadline to send an article. The earlier you submit, the greater your chance of being published and reaching a wider audience. As with most things in the Army, there is a process for getting your work published. Part of that process entails that I submit a "packet" to Line of Departure once your article is finalized (to be published online). This is done on an individual, ongoing basis. There is no longer a need to wait until the established deadline to send your article. Although a deadline is established for the Fall 2026 Army Communicator (Sept. 4), I urge you to submit before then if possible. The submission guidelines published below – and on Line of Departure – **must be followed** to be considered for publication.

Lastly, I can't emphasize enough the importance of having a photo (or several) to accompany articles. Not only is it a requirement for Line of Departure, but it draws readers in. An action photo is best, when possible. There are times when I can assist with searching for a photo, but the best ones are tailored to the article itself – which typically equates to it being taken in the author's area of operation, in which case, I cannot always assist.

Not sure where to begin? Check out How to Write an Article in Military Review.

And as always, please don't hesitate to reach out directly to me (email preferred)!

Submission guidelines

Articles need to be sent in Word. Photos and graphics must be attached **separately (*not embedded*** in Word**).** Include a description of each photo/graphic along with the rank, full name, and unit of who took the photo (created graphic, illustration, etc.). Acronyms **must be spelled out** on first reference, with the abbreviation of the term acceptable on subsequent reference. Between 500 and about 2,000 words per article is ideal. This helps ensure a minimum of one page and maximum of four pages in publication layout (depending on photos, etc.). Citations/references must follow **APA** Style.

Fall 2026 deadline: Sept. 4

Building an Enduring, Resilient Soldier

Chaplain's Corner

Chaplain (Maj.) Glen Thompson
U.S. Army Signal School

As an Ethics chaplain assigned to the U.S. Army Signal School, I spend my days walking the line between the sacred and the synthetic – where the next generation of Signaleers learns to build, operate, and defend the military's most critical communication infrastructures. Yet, the most vital network we build at this institution is not composed of fiber optic cables, routers, or equipment. The truly enduring network is of the human domain – forged from the resilient character and unwavering ethics of our Soldiers.

We build resilient Soldiers rooted in strong ethics, recognizing that **trust** is the absolute bedrock of the Army foundation. Army doctrine explicitly establishes trust as the bedrock upon which all cohesive teamwork and decentralized execution – the core of mission command – are built.

Trust is the center of gravity for every effective Army leader, and for Signalers it becomes even more critical. ADP 6-22 frames trust as the foundation of the Army Profession, the essential bond that allows Soldiers to operate confidently in complex, high-pressure environments. For Signal Soldiers, who safeguard networks, enable mission command, and keep the force connected, trust is not just a leadership concept. It is a combat multiplier**.**

Building trust begins with **character,** the first of the Army's leadership requirements. Signalers earn trust when they demonstrate integrity in every action, from protecting sensitive information to maintaining communications security. When Soldiers see leaders consistently uphold standards, even when no one is watching, they gain confidence that their leaders will do the right thing under stress. This moral consistency becomes the bedrock of resilience.

Competence is the second pillar. Army Doctrine Publication (ADP) 6-22 emphasizes that leaders build trust by demonstrating the ability to perform their duties to a high standard. In the Signal Corps, competence means mastering rapidly evolving technologies, troubleshooting under pressure, and delivering reliable communication in all conditions. When a Signaleer proves they can keep the network alive in chaos, they strengthen the team's belief in the mission and in each other. Competence fuels resilience by reducing uncertainty and empowering disciplined initiative.

Commitment completes the three Cs. Leaders show commitment by investing in their Soldiers' development, advocating for resources, and demonstrating genuine care for the team's well-being. ADP 6-22 notes that trust grows when Soldiers believe their leaders are dedicated to their success. For Signaleers, this means creating a climate where learning is encouraged, mistakes become opportunities, and every Soldier feels valued. Such climates produce resilient teams capable of adapting to adversity.

Ultimately, trust transforms a group of individuals into a cohesive, resilient Signal formation. It enables decentralized execution, fosters psychological safety, and strengthens the shared belief that the team can overcome any challenge. When Signaleers trust their leaders, their equipment, and each other, they become more than technical experts – they become the connective tissue of the Army's operational success.

Beyond Connectivity: Measuring Mission Command Through Decision Velocity

'The voice to give command'

Sgt. Jermaine S. Sayers
551st Signal Battalion

"We give our Army the voice to give command."

The Signal Corps has fulfilled this mission by connecting commanders to formations across the battlefield for over 160 years. From signal flags and torches during the Civil War to satellite communications spanning the globe, signal Soldiers have enabled command and control in every major conflict. However, connectivity itself is not enough in this new era of multidomain operations, artificial intelligence (AI), and contested communications environments.

Communication success within the Army is often assessed using metrics including network availability, bandwidth, uptime, and coverage. Athough these measures continue to be relevant, they do not determine the key issue facing modern commanders: Does the network facilitate faster decision-making and execution than the enemy can achieve?

Army doctrine states that successful execution requires Army forces to make and implement effective decisions faster than enemy forces (Department of the Army, 2019). If victory hinges on effectiveness and pace of decision-making, decision velocity rather than connectivity alone should serve as the primary measure of mission command.

Purpose Behind Connectivity

"The Signal Corps March" captures the Corps' enduring purpose:

From flag and torch in the Civil War,
To signal satellites afar.
We give our Army the voice to give command,
On battlefield or global span.

The key phrase is not "signal satellites afar;" the key phrase is "the voice to give command." The value of communication lies not in communication itself, but in its ability to facilitate and command control.

Every radio, satellite link, tactical network, and command post exists to help commanders understand situations, issue guidance, synchronize operations, and accomplish missions. C2, in accordance with Army Doctrine Publication 6-0, enables commanders to comprehend situations, make decisions, direct actions, and lead forces toward mission accomplishment (Department of the Army, 2019). Consequently, the measure of effective C2 is not solely the transmission of information but the decisions and actions that are enabled as a result of information.

Staff Sgt. Jonathan Nichols, 15th Signal Brigade, demonstrates a signaling technique using a Wig-Wag flag. The Wig-Wag systems dates back to 1860, when Army Maj. Albert Myer proposed that the Army use his suggested means of communication in battle. (Photo by Spc. Samantha Powers, Cyber Center of Excellence Public Affairs)

More Than Networks

Mission command is the Army's approach to C2 that empowers subordinate decision-making and decentralized execution appropriate to the situation (Department of the Army, 2019). This philosophy depends on mutual trust, shared understanding, disciplined initiative, and commander's intent. Mission command is not built upon technology alone; it is built upon people and their ability to make decisions under conditions of uncertainty.

Studies on military command indicate that during chaotic operations, effective leaders navigate pressure by utilizing sense-making, experience, cohesion, and trust (Tyler & Tyler, 2015). This reinforces that while informational networks facilitate the process, they cannot substitute for fundamental human decision-making. Similarly, research conducted under the Tactical Decision Making Under Stress program found that decision quality breaks down when the volume of information presented exceeds a person's capability of processing it (Hseu et al., 1992).

Staff Sgt. James Castilleja and Spc. Isaac Craig, 5th Battalion, 3rd Long Range Fires Battalion, 1st Multi-Domain Task Force, deploy tactical fiber -optic cable to establish secure communications between the Battery Operations Center and the Transporter Erector Launcher during training operations. (Photo by Sgt. Steven Andrade, 5-3 LRFB)

In essence, more information does not automatically lead to better decisions. This distinction is critical as a network that provides unlimited access to data but overwhelmed decision-makers may actually reduce operational effectiveness. Conversely, a network that provides commanders with relevant and actionable information can significantly improve mission outcomes.

Understanding Decision Velocity

Decision velocity is the method of how quickly and effectively decisions are made and executed within an organization (Jafferi, 2025). Organizations that have high decision velocity are more adaptive, more innovative, and better positioned to capitalize on opportunities. Conversely, slow decision velocity increases friction, delays action, and allows competitors to gain advantages (Jafferi, 2025).

The concept extends beyond the business world. The GitLab Handbook describes decision velocity as the ability to increase both the quality and quantity of decisions made within a given period of time while maintaining a bias toward action (GitLab, n.d.). This principle directly supports the Army's mission command philosophy.

The role of mission command is to empower subordinate leaders to act within the commander's intent rather than waiting for detailed guidance. Faster, high-quality decisions at lower echelons increase agility and responsiveness throughout the force.

Future Battlefield

The future battlefield will be saturated with sensors, intelligence feeds, autonomous systems, and AI. Commanders will have access to more information than at any point in military history. However, the challenge is not obtaining information; the challenge is transforming information into understanding.

Bhatnagar (2026) argues that modern warfare increasingly relies on algorithmic systems that influence decisions at speeds beyond human comprehension. While these systems provide advantages in speed and scale, they also introduce risks such as overreliance on automated recommendations and the potential erosion of human judgment.

On the same coin, Matei and Reed (2025) argue that AI can enhance mission command by condensing large volumes of battlefield data into decision-quality information. Their research emphasizes information asymmetry, where detailed information flows upward while concise, actionable guidance flows downward. This process enables commanders to focus on decisions rather than data management. These findings suggest that future success will depend less on moving more information and more on delivering the right information to the right decision-maker at the right time.

Beyond the Network

Creel and Torrence (2025) argue that the Signal Corps must evolve from being a provider of connectivity to becoming an enabler of decision dominance. They contend that the Army's success depends on its ability to see, decide, and act faster than its adversaries. This perspective represents a significant shift in how signal Soldiers should view their role. Rather than focusing solely on technical performance metrics,

signal leaders should consider how communications systems contribute to operational outcomes.

Questions worth asking include: **"**Did the network accelerate decision-making?" "Did it improve shared understanding?" "Did it support disciplined initiative?" "Did it reduce decision-making timelines?" "Did it contribute to mission accomplishment?"

These questions better reflect the purpose of communications within mission command.

How to Measure Decision Velocity

Decision velocity can become a significant mission command metric. Signal leaders can transcend measuring network performance alone by assessing how communication systems contribute to operational decisions. The metrics could include the time interval between information collection, commander awareness, dissemination of orders/decision issuance and subordinate acknowledgment, also the speed at which units execute directed actions. During training exercises and operations, signal leaders can compare these timelines against mission outcomes to identify bottlenecks that affect decision making. The evaluation of how rapidly information is transformed into decisions and decisions into actions can determine the efficiency of communication systems for commanders to understand, decide, and act faster than adversaries. This approach aligns technical network performance with the ultimate purpose of mission command: creating decision advantage on the battlefield.

Conclusion

The Signal Corps has always provided the Army with the voice to give command, yet connectivity has never been the end state. Army doctrine emphasizes that successful execution depends upon making and implementing effective decisions faster than enemy forces (Department of the Army, 2019). Modern research on decision-making, mission command, and AI reinforces this principle by demonstrating that the value of information lies not in its volume but in its ability to support action (Matei & Reed, 2025; Tyler & Tyler, 2015).

As warfare becomes increasingly data-driven, the Army must look beyond traditional connectivity metrics and focus on what truly matters: decision velocity. The greatest contribution of the Signal Corps is not merely connecting systems. It is enabling commanders and formations to understand, decide, and act faster than any adversary.

References

Bhatnagar, P. (2026). *The algorithmic battlefield: How AI is redefining modern warfare*. Technical Disclosure Commons.

Creel, J. R., & Torrence, J. J. (2025). *Beyond the network: The Army Signal Corps and the future of warfare*. Military Review Online Exclusive.

Department of the Army. (2019). *Mission command: Command and control of Army forces* (ADP 6-0). Headquarters, Department of the Army.

GitLab. (n.d.). *Decision velocity*. GitLab Handbook.

Hseu, J. K., Volpe, C. E., Cannon-Bowers, J. A., & Sales, E. (1992). *A performance assessment task for examining tactical decision making under stress*. Naval Training Systems Center.

Jafferi, T. (2025). *The decision velocity advantage: How trust and clear values drive competitive edge*. Happily.ai.Matei, S. A., & Reed, K. P. (2025). *Mission command's asymmetric advantage through AI-driven data management*. Parameters, 55(4).

Tyler, I. B., & Tyler, A. C. (2015). *Decision making in chaos*. Naval Postgraduate School.

Resilience Through Redundancy: Closing the Company-Level Communications Gap

The enduring Signaleer

Maj. Jonathan Steel
3rd Mobile Brigade, 101st Airborne Division (Air Assault)

The enduring Signaleer builds resilient networks not by preventing failure, but by ensuring the formation can fight through it. During Joint Readiness Training Center (JRTC) rotation 26-06, the 3rd Mobile Brigade (MB), 101st Airborne Division (Air Assault), faced simulated adversary cyber and electronic warfare attacks – dubbed "Operation Space Jam – that disabled commercial satellite communications (COMSATCOM).

Although the brigade maintained command and control (C2)through transport diversity and active network management, demonstrating that resilience is achievable when redundant systems exist, the exercise exposed critical gaps: limited military satellite communications (MILSATCOM) below brigade, and complete absence of robust beyond line-of-sight (BLOS) high-bandwidth connectivity at the company level.

This article examines how 3rd MB responded to contested conditions, identifies organizational vulnerabilities, and proposes solutions centered on proliferated low Earth orbit (pLEO) satellite terminals for companies and stratospheric aerial retransmission.

Testing Resilience Under Fire

The 3rd MB employed organic On-the-Move Network Nodes (ONN) and four Division Network Node (DNN) At-the-Quick-Halt (ATQH) systems from the division signal battalion, all equipped with the Seeker (SKR) software suite. SKR's multi-transport input and automated load balancing supported up to four simultaneous internet transports, enabling the brigade to sustain C2 during repeated cyber and electromagnetic interference events.

During three separate "Operation Space Jam" attacks, Starshield – the primary COMSATCOM transport – was forced offline, shifting traffic to Long-Term Evolution (LTE)-based Mobile Broadband Kits (MBK). In the first two events, the Brigade Forward Command Post used the DNN Tampa MILSATCOM dish. The node aligned to the Main Command Post (MCP) was decentralized to support the new Alternate Logistics Operations Center (ALOC) co-located with the Brigade Support Area, leaving the MCP without MILSATCOM support.

In the third event, the MCP operated with the rotation's most robust communication architecture, trunking the ONN Colorless (XLESS) Core to the DNN via the ATQH organic MILSAT transport without significant reconfigurations on the nodes while maintaining services at reduced bandwidth.

SKR's telemetry system enabled rapid detection and ensured service continuity across C2 nodes. The brigade completed its fastest Joint Spectrum Interference Report (JSIR) battle drill in 33 minutes; 22 minutes faster than the previous JRTC record. Bandwidth virtualization and active load balancing increased resilience against jamming and transport denial, distributing traffic and sustaining essential C2 under degraded conditions.

The Limits of Borrowed Resilience

Despite operational success, two structural risks constrain endurance under contested conditions.

First, the brigade lacks organic MILSATCOM capacity, relying instead on the division signal battalion's Tampa dishes, typically limited to two brigade nodes habitually aligned. This creates single points of failure and leaves battalions and companies without redundant MILSATCOM paths. Second, ONN and ATQH C2 nodes depend on SKR licenses that are lost during server failures, rendering nodes inoperable and imposing reconstitution lead times exceeding 48 hours.

These risks are magnified by contemporary adversaries who blend presence-based intrusions with event-triggered effects targeting C2 and logistics networks. The brigade's outcomes demonstrate progress toward an integrated defensive posture, but structural gaps remain. While the formation can fight through transport denial with graceful degradation – preserving priority C2 functions and sustaining decision-making tempo – limited MILSATCOM allocation below brigade and dependence on SKR licenses pose real concerns. Localized jamming or server faults could lead to operational pauses if multiple nodes are contested for prolonged periods.

Where Resilience Ends

While brigade and battalion echelons demonstrated resilience through redundant transport layers, companies remained tethered to detectable, jammable systems. Modern maneuver companies operate under unprecedented information requirements, maintaining near-real-time common operational pictures (COP) through Android Tactical Assault Kit (ATAK), Battle

Command Sustainment Support System (BCS3), and Logistics Tactical Assault Kit (LOGTAK) – all requiring continuous high-bandwidth connectivity.

Current company-level BLOS communications rely on four primary systems: LTE-based MBKs, Mounted Mission Command (MMC), Mobile User Objective System (MUOS), and High Frequency (HF) radio. Of these, only MBK provides sufficient bandwidth to support COP applications. Tactical Scalable Mobile Ad Hoc Networks (TSMANETs) excel for internal position location information and voice communications but cannot meet data-intensive application throughput requirements. This creates a critical vulnerability: LTE is inherently susceptible to threat interference and potentially exposes its' users.

During Operation Space Jam attacks, brigade and battalion CPs maintained operations through redundant MILSATCOM and COMSATCOM paths, but companies lacked equivalent resilience. When commercial and LTE transports are contested, companies lose all high-bandwidth connectivity. This asymmetry creates operational risk: companies cannot maintain the COP, pass targeting data at tempo, or synchronize logistics when dispersed in contested electromagnetic environments.

Path Forward

Small pLEO terminals at the company level provide resilient, mobile, independent communication solutions critical to maintaining C2 in distributed operations. They resist jamming through frequency hopping and beam steering, deploy rapidly, and integrate with existing networks. Critically, they provide the bandwidth needed to sustain COP applications while maintaining low electromagnetic signatures and offering low probability of intercept/low probability of detection (LPI/LPD) characteristics.

Aerial Retransmission Reimagined

Beyond transport diversity at the company level, the 3rd MB tested high-altitude balloons for aerial retransmission during JRTC 26-06. In previous 101st Airborne Division JRTC rotations, long-endurance unmanned aerial platforms provided up to four hours of coverage but were grounded more often than airborne due to weather or contested airspace. To address these limitations, 3rd MB tested high-altitude balloons briefed to provide 24 to 72 hours of coverage above 60,000 feet, well above weather and Class A airspace.

Over eight flights totaling 26 hours – five TSM relay flights and three SILVUS flights – provided approximately 12 hours of aerial extension over the training area. The highest altitude reached during this rotation was over 75,000 feet during the second night of flight. Through this, the brigade established a link from the Brigade Forward Command Post in Fullerton box to reach back to the Logistics Support Battalion in Alexandria, Louisiana. The tests yielded mixed results. SILVUS data backhaul tests failed mainly due to improper antennas and possibly insufficient power. Expected long-duration coverage lasted only 90-minute windows, likely due to stratospheric winds and differences between flown and advertised heights.

Analysis of JRTC 26-06 operations indicates aerial retransmission offers significant potential for network extension in contested environments. A maneuverable, long-range drone operating in the stratosphere could mitigate challenges posed by weather and contested airspace. For the enduring Signaleer, operationalizing the stratospheric layer represents an opportunity to extend resilient communications beyond terrestrial and orbital system constraints. A maneuverable, long-endurance stratospheric platform equipped with TSM retransmission and high-bandwidth data backhaul could provide persistent aerial extension for dispersed companies in contested environments – bridging the gap between line-of-sight tactical networks and BLOS satellite transport.

Priority Actions for the Enduring Signaleer

To build resilience from the company up, the Army must address three priority actions:

1. Field organic MILSATCOM redundancy at echelons below brigade. Provide at least one additional MILSATCOM-capable path to Main and Forward Command Posts and evaluate redundancy for battalion nodes. This reduces single points of failure and ensures graceful degradation during transport denial events.

2. Distribute LPI/LPD high-bandwidth BLOS transport to the company level. Acquire small pLEO terminals – one per maneuver company and two for forward resuscitation and critical care – through the United States Space Force Commercial Satellite Communications Office (USSF CSCO) contracting pathways. Integration must enforce physical and logical separation from NIPRNet and SIPRNet while enabling multi-transport load balancing at battalion and brigade levels.

3. Operationalize the stratospheric layer for aerial retransmission. Invest in maneuverable, long-endurance stratospheric platforms capable of hosting TSM retransmission and high-bandwidth data backhaul. These platforms mitigate weather and airspace limitations while providing persistent aerial extension for dispersed formations.

Additionally, establish a SKR license continuity-of-operations plan: pre-approved spare licenses, offline

license escrow, hot-standby license servers, and scripted re-licensing drills to avoid long reconstitution times after server or node losses.

Conclusion

Resilience is not an abstraction. It is the practical ability to keep essential C2 moving when the spectrum turns hostile. JRTC 26-06 demonstrated that with transport diversity, active management, and MILSATCOM at key nodes, formations can fight through denial while maintaining tempo. The brigade's 33-minute Joint Spectrum Interference Resolution cycle time and sustained operations during three separate jamming events prove resilience is achievable but only where redundancy exists. To make that resilience enduring where it matters most – at the company – the Army must close the BLOS bandwidth gap with LPI/LPD, high-bandwidth solutions tailored for maneuver. Companies face the same contested electromagnetic environment, the same adversary electronic warfare capabilities, and the same mission-essential bandwidth requirements as the brigade and battalion – but lack the transport diversity to fight through denial. Distributing small pLEO terminals to companies and operationalizing the stratospheric layer for aerial retransmission ensures that resilience built at brigade and battalion echelons extends to the formations that close with and destroy the enemy.

The enduring Signaleer ensures that no formation – regardless of echelon – fights blind, isolated, or unable to share information that enables lethality and survivability. Building resilient networks from the company up is not simply an upgrade; it is a critical investment to maintain C2 in the face of evolving battlefield realities.

Author

Maj. Jonathan Steel is the signal officer (S6) for 3rd Mobile Brigade, 101st Airborne Division (Air Assault), at Fort Campbell, Kentucky. Steel led brigade communications operations during Joint Readiness Training Center rotation 26-06, where his team achieved the fastest Joint Spectrum Interference Resolution battle drill in JRTC history at 33 minutes.

Previously, Steel served as the network operations officer-in-charge for the 101st, where he helped implement the division's C2 modernization and developed communications architecture for large-scale, long-range air assault operations. He has also held key positions with 25th Infantry Division and 10th Mountain Division. Steel holds a master's degree from Command and General Staff College at Fort Leavenworth, Kansas.

Employing the Right Technical Expert: Why Signal WOs Specialization Matters

Team effort

Regimental Chief Warrant Officer 5 Willie Newkirk
U.S. Army Signal School

The Army's operational environment has changed dramatically. Large-scale combat operations, persistent competition below armed conflict, and increasingly capable peer adversaries have transformed how the Army approaches command and control, network operations, and cyberspace defense. Success in multi-domain operations now depends on an Army network that is not only operational, but resilient, secure, and defensible under continuous pressure.

The Department of Defense Information Network (DoDIN) serves as the foundation for mission command, data sharing, operational synchronization, and joint convergence. As Army doctrine makes clear, the network is no longer merely an enabling capability; it is a warfighting platform. Commanders depend on reliable communications, protected data, secure enterprise services, and resilient infrastructure to maintain decision advantage across all domains.

Building and defending that capability requires more than technology. It requires experienced technical leaders capable of integrating complex systems, managing operational risk, and translating technical capabilities into combat power.

FM 3-12 explains Army cyberspace and electronic warfare operations fundamentals, terms and definitions.

Signal warrant officers serve as the Army's senior technical experts and trusted advisors in this environment. They bridge the gap between technology and operations, ensuring commanders can leverage network and cyberspace capabilities to achieve mission success. However, as the Army continues to modernize, misconceptions persist regarding the roles and employment of signal warrant officer specialties.

The Army deliberately developed the Data Operations Warrant Officer (255A), Network Operations Warrant Officer (255N), and Cyberspace Defense Warrant Officer (255S) as complementary but distinct technical specialties. Each specialty provides unique capabilities that contribute to network resiliency, operational readiness, and mission command. Understanding these distinctions is essential for commanders and leaders responsible for employing technical talent effectively.

The Importance of Specialization

Modern Army networks are extraordinarily complex. Tactical and enterprise environments now rely on interconnected transport systems, cloud-enabled services, virtualization platforms, identity management systems, cybersecurity frameworks, and defensive cyberspace operations. These capabilities must function continuously while facing persistent threats from sophisticated adversaries.

The Army does not develop technical mastery by accident. Signal warrant officer specialization reflects a deliberate effort to build deep expertise aligned with operational requirements across the cyberspace domain. While all signal warrant officers share a common technical foundation, each specialty develops advanced competencies in a specific operational discipline. This specialization matters because network operations, enterprise services management, cyberspace security, and cyberspace defense require different skill sets, different training pathways, and different operational experiences.

Technical generalization may appear to offer flexibility, but over time it often creates inefficiencies, increases risk, and reduces effectiveness. The Army's technical advantage depends upon placing the right expertise in the right role. Proper employment of signal warrant officers ensures commanders receive the technical leadership necessary to build, sustain, secure, and defend the network capabilities that enable mission command.

The 255N: Building the Foundation

The Network Operations Warrant Officer (255N) serves as the Army's expert in network operations,

transport integration, and digital infrastructure modernization. Their focus extends beyond traditional routing and switching to designing, securing, and strengthening the architectures that support the Army Unified Network.

The 255N designs and manages enterprise routing and switching architectures, oversees tactical and strategic transport integration, implements secure network configurations, and ensures infrastructure remains resilient and available. In practical terms, the 255N ensures data can move reliably from one point to another across the DoDIN. Mission command systems, cloud services, voice communications, and tactical data exchanges all depend on the infrastructure they design and maintain. Their work is critical in contested environments where adversaries seek to disrupt communications, degrade network availability, and create friction within command-and-control systems.

Through redundancy, segmentation, failover design, dynamic routing, and rapid restoration, the 255N sustains resilient mission command and preserves connectivity under pressure. They implement secure architecture, implement and manage firewalls, enforce network security standards, and operationalize zero trust principles to protect from exploitation. Simply stated, the 255N secures the pathways through which data travels. Without reliable transport infrastructure, commanders lose the ability to communicate effectively, synchronize operations, and maintain situational awareness. The 255N ensures those pathways remain operational under any conditions.

The 255A: Sustaining Services

The Data Operations Warrant Officer (255A) concentrates on managing services, applications, systems, cloud environments, cyberspace security, and data that enable operations. As the Army shifts to data-centric operations, the 255A serves as the Army's expert in data integration, systems management, platform operations, identity management, virtualization, storage environments, and cybersecurity. Their work makes data visible, accessible, understandable, linked, trustworthy, interoperable, and secure at all echelons. Their responsibilities encompass the services that commanders and staff rely on every day to plan, coordinate, and execute operations.

From a cyber perspective, unlike the 255S, whose mission focuses on cyberspace defense, the 255A concentrates on risk reduction and operational readiness (cybersecurity). Through configuration management, vulnerability remediation, compliance enforcement, identity governance, and security baseline implementation, the 255A reduces attack surfaces and strengthens enterprise resiliency. Their work is preventative in nature. By maintaining secure and compliant systems, they help ensure networks remain capable of supporting operations even under adverse conditions.

In many ways, the 255A serves as the steward of the Army's enterprise environment. Their expertise ensures that critical services remain available, secure, and capable of supporting mission requirements across the force.

The 255S: Defending Against the Threat

The Cyberspace Defense Warrant Officer (255S) provides a fundamentally different capability than either the 255A or the 255N. Where the 255A and 255N operate within DoDIN Operations, the 255S operates within Defensive Cyberspace Operations–Internal Defensive Measures (DCO-IDM). The 255S is the local defender. Their mission is not to secure systems, but to actively defend networks and key cyber terrain against malicious cyber activity. The 255S focuses on threat detection, incident response, cyber threat analysis, hunt operations, and intrusion mitigation. Their work is informed by intelligence, adversary behavior, and network telemetry rather than administrative compliance requirements. This distinction is important because cybersecurity and cyberspace defense are not synonymous.

Cybersecurity seeks to reduce risk through policies, configurations, governance, and preventative controls. Cyberspace defense seeks to identify, analyze, and defeat adversaries actively operating in cyberspace.

A system may be fully compliant with cybersecurity standards and still become the target of a sophisticated cyber intrusion. When that occurs, the 255S becomes essential. The Cyberspace Defense Warrant Officer investigates indicators of compromise, analyzes malicious activity, identifies adversary tactics and techniques, and coordinates defensive actions to contain and mitigate threats. Their efforts preserve operational continuity by preventing adversaries from achieving their objectives within the network.

As cyber threats continue to evolve, commanders increasingly depend on the 255S to provide technical expertise capable of defending mission-critical systems against active attack.

A Team Effort

Although each specialty serves a distinct purpose, none operates in isolation. Building, managing and defending a resilient network requires synchronized efforts across infrastructure operations, services management, cybersecurity governance, and cyberspace defense.

The 255N, 255A, and 255S each contribute unique capabilities that collectively enable mission command. Consider a division operating in a contested environment. During a critical operation, commanders begin experiencing degraded access to mission command

systems. Authentication services become unreliable, network performance deteriorates, and reports indicate potential malicious activity. Addressing this challenge requires expertise from all three specialties:

The 255N evaluates network transport infrastructure, routing stability, segmentation controls, and connectivity issues to determine whether infrastructure degradation is affecting availability.

The 255A examines authentication systems, directory services, virtualization platforms, and applications to identify service disruptions or system failures that may be contributing to the problem.

The 255S investigates indicators of compromise, analyzes suspicious activity, conducts threat hunting operations, and coordinates defensive actions to determine whether adversaries are actively operating within the environment.

Each warrant officer views the problem through a different operational lens. Together, they provide commanders with a comprehensive understanding of the situation and enable an effective response.

The same principle applies during modernization initiatives. The 255N designs resilient network architecture, the 255A integrates services and identity management solutions, and the 255S ensures that threat considerations and defensive monitoring are incorporated into the design. Success depends upon synchronization among all three specialties.

Conclusion

The Army's ability to fight and win future conflicts depends on resilient networks, secure services, protected data, and active defense against increasingly capable adversaries. Signal warrant officers remain central to that mission.

The 255A, 255N, and 255S specialties represent deliberately developed technical capabilities aligned to distinct operational requirements across DoDIN Operations and Defensive Cyberspace Operations – Internal Defensive Measures. Together, they provide commanders with the expertise necessary to build, operate, secure, and defend the network capabilities that enable mission command.

As the Army continues its transformation toward multi-domain operations, leaders must understand that these specialties are complementary; they are not interchangeable. Proper employment of technical expertise directly influences operational readiness, network resiliency, incident response effectiveness, and the Army's ability to achieve information advantage during competition and conflict.

The enduring Signaleer is defined by technical mastery, operational adaptability, and a commitment to mission success. Building, operating, securing, and defending the Army network requires specialized expertise, synchronized operations, and technical leaders capable of translating complexity into operational advantage.

The Army cannot afford to generalize highly specialized technical talent. Success in future operations will depend on employing the right technical experts in the right roles at the right time.

THE QUIET PROFESSIONAL

Author

Chief Warrant Officer 5 Willie L. Newkirk is the 8th Regimental Chief Warrant Officer at the U.S. Army Signal School, Fort Gordon, Georgia, where he previously served as technical director of the school. His military career began on Sept. 11, 1996, as an enlisted Soldier, during which he served in a variety of roles across both operational and institutional Army assignments. Newkirk was appointed as a warrant officer in May 2005 after completing Warrant Officer Candidate School, and upon graduation from the Warrant Officer Basic Course, he was awarded military occupational specialty 251A (Information Systems Technician). More details on Newkirk's military background can be found here.

AESMP Raptor DB Pro: Making Life As an Army Communicator More Efficient

Asset management

John Meister
Army Enterprise Service Desk-Worldwide

On May 1, 2026, ServiceNow fielded a significant upgrade to the U.S. Army Enterprise Service Management Platform (AESMP) with the integration of Raptor DB Pro. At its core, Raptor DB Pro is a high-speed, artificial intelligence (AI) and machine learning (ML) enabled, scalable database engine specifically designed to enhance data-driven decision making and efficient information sharing. Raptor DB Pro can easily handle large and complex data sets with efficiency and accuracy to enable information technology (IT) leaders to operate with data and tools not previously available providing advanced solutions to problems prevalent in today's environment.

Changing the Scope of Asset Management

In today's challenging environment, keeping track of vast amounts of IT hardware and software needs at various levels within both the strategic and tactical formations of the Army is a nearly impossible task. To address these issues, leaders and Soldiers spend significant time tracking down specific machines and devices on the network to comply with property accountability guidance and addressing network compliance issues. However, with the availability of Raptor DB Pro on the AESMP management system readily available across the Army, there is a solution to making those challenges much easier and at no cost to the organization.

Hardware Asset Management (HAM)

AESMP enhanced with Raptor DB Pro allows asset managers and users to conceptualize thousands of hardware devices and configuration items (CI) on enterprise and tactical networks in a matter of seconds. Simply using the aspects of Raptor DB Pro, a user can identify hardware by location, serial number, device type, life cycle information and user compliance by simply checking the Asset management dashboard imbedded within Raptor DB Pro.

Additionally, Raptor DB Pro is designed to filter out duplicate data reducing reconciliation issues which significantly decrease the time needed to conduct required inventories and property book actions.

Software Asset Management (SAM)

For software management, Raptor DB Pro can easily identify devices that are not within software compliance and pinpoint them for maintenance. Furthermore, Raptor DB Pro allows users to query software licenses, identify expiration dates, forecast renewal timeframes, and proactively give organizations time to address these challenges before they will impact the network.

Lifecyle Management and Replacement:

Utilizing the Raptor DB Pro enhanced AESMP system, organizations can now easily capture lifecycle management data needed to determine replacement timelines and priorities.

The AESMP will rapidly provide device type, specific dates for replacements and the duration the device has been on the network. This capability also allows organizations to capture price and cost information that enables leaders to accurately predict costs and budget for future lifecycle replacement needs.

Meeting Needs of the Modern Army

With the successful deployment of Raptor DB Pro within the AESMP system, the ability for leaders to meet network compliance and security requirements has never been easier.

Army communicators consistently manage various IT level threats and enterprise network level orders and directives from Defense Information Systems Agency (DISA), U.S. Army Cyber Command (ARCYBER), and U.S. Army Network Enterprise Technology Command (NETCOM).

Requirements from these commands are many times vast and contain thousands of configuration items which have an impact on organizational resources and timelines.

Utilizing this new technology within AESMP, units and organizations can accomplish these requirements with a vastly improved efficiency. Raptor DB Pro can process enormous amounts of data in a fraction of the time required with previous network tools, enabling units and organizations to query large amounts of data to include the installation and strategic levels of the Army.

AESMP/Raptor DB Pro Training

AESMP is fielded across the Army at no cost to the unit or organization. This applies to all required training for users on the platform. AESMP/Raptor DB Pro training is conducted via the Army Training Information System (ATIS) in an online format. Now when applying for AESMP privileges required training, the use of Raptor DB Pro in ATIS is included. Training is straight forward and efficient in teaching users the techniques to utilize all the tools now available. This training is available for any Soldiers, commanders and Army communicators designated to serve as asset managers for property and inventory processes.

Make Life Easier

Now that Raptor DB Pro is available within AESMP, leaders and commanders have a readily available tool to ease the day-to-day challenges of asset management. Utilizing this cutting-edge database engine – which enhances previous capabilities by integrating AI and ML – significantly increases your ability to visualize and manage the network.

As the Army develops, solutions like Raptor DB Pro will remain at the core of its IT enterprise mission to protect the network and create fast, effective visibility of enterprise challenges.

Author

John Meister is a retired senior Army officer who previously served in leadership positions at brigade, Corps G6 and battalion levels across the Army for over 24 years. He currently serves as the Communications Principle for the AESMP program in support of ARCYBER and NETCOM for SAIC.

Parker Hitt: An Unsung Pioneer in the Military

Book review

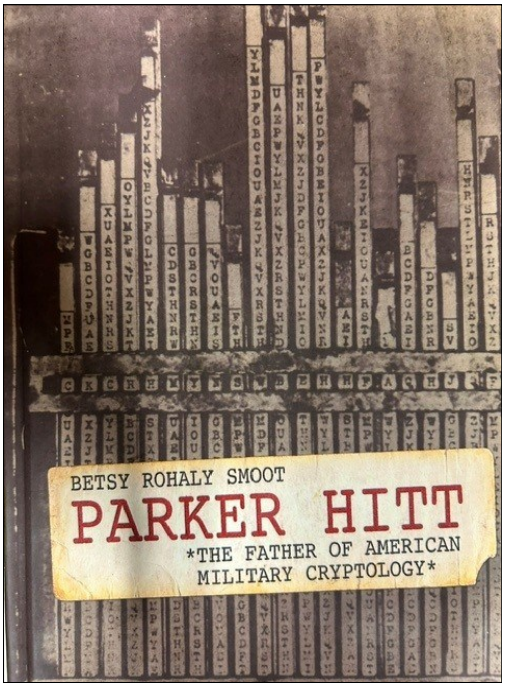
Ivan Zasimczuk
U.S. Army Signal School

In the book "Parker Hitt: The Father of American Military Cryptology," author Betsy R. Smoot delivers a well-researched and insightful biography of an unsung pioneer in military communications encryption. The book chronicles the extensive and influential career of Parker Hitt, a foundational figure in the development of the U.S. Army's signals intelligence (SIGINT) and cryptographic capabilities.

The structured chronology spans across 11 chapters and narrates Hitt's life from his birth in 1878 to his death in 1971 and concludes with a legacy section. Smoot presents Hitt as a relentless innovator and pivotal leader present at the very inception of American military cryptology.

Smoot's story begins in 1898, when Congress authorized a 125,000-man volunteer force and Hitt, a 19-year-old third-year student, dropped out of Purdue University to join the Army. Although Hitt missed combat in the Spanish-American War, in September 1899, he earned a commission and deployed to the Philippines.

The text's initial chapters cover his early service – including capturing insurgents and conducting earthquake relief in San Francisco – before transitioning to a significant portion dedicated to his time at the Army Signal School. There, Hitt's inventive genius flourished. Smoot details his creation of a new cipher system, his design of an upgraded switchboard, and his authorship of the semifinal "Manual for the Solution of Military Ciphers." Before hitting her stride in the chapters about World War I, Smoot effectively outlines the formative assignments preceding that culminating period.



"Parker Hitt: The Father of American Military Cryptology" is a biography of an unsung pioneer in military communications encryption. (Courtesy image)

Hitt attended flight school in San Antonio. He wrote and presented a pivotal paper, "Enciphering and Deciphering Device," which explained his newly designed cylindrical tool that later became the basis for the Army's M-94 cipher device. He also designed a telescopic rifle sight and an air-cooled machine gun.

Following service on the Mexican border, Hitt deployed to France in May 1917. His expertise was immediately recognized and led to his appointment as chief signal officer in July 1918 for the newly created First Army. The narrative highlights his work establishing the first American Expeditionary Forces (AEF) code room; his battles for communication resources; his championing of the female telephone operators affectionately known as the "Hello Girls;" and his implementation of radio deception tactics.

The post-World War I period covers Hitt's friction with the chief signal officer, George O. Squier; his service on the Army War College faculty; and his eventual retirement in 1928 to join International Telephone and Telegraph (IT&T).

Equally interesting – though troubling – Hitt's post-war participation in domestic surveillance operations against suspect organizations and private citizens. While these activities were a natural, if controversial, extension of his intelligence collection against foreign entities, they represent clear violations of civil rights driven by the era's Red Scare and fears of subversive activities. Though such actions may have been less controversial than they are today, they represent a dangerous use of the Army's capabilities against American citizens.

The final chapters detail Hitt's recall to service as a Signal Corps officer from 1940-1943, when he reached the mandatory retirement age of 65.

Ultimately, the book provides a thorough account of a man whose work fundamentally shaped American military intelligence and SIGINT collection. Smoot successfully positions Hitt as a key architect of systems and methods that remained crucial in cryptology for decades.

Smoot's coverage of Hitt's wartime service and numerous technical innovations are the undeniable highlights of the work. The narrative flow is occasionally interrupted by peripheral minutiae – such as the Hitt family's frequent relocations, housing situations, and minor daily routines. While these domestic details

succeed in humanizing Hitt, readers might find that they distract from Smoot's core military and historical focus.

Despite these pacing flaws, Parker Hitt is highly recommended for members of the Signal, Military Intelligence, and Cyber branches, as well as military professionals across the joint force. Beyond branch-specific technical history, the book captures an underlying spirit of innovation and curiosity that holds broad appeal. Pairing this work with "George Owen Squier: U.S. Army Major General, Inventor, Aviation Pioneer, Founder of Muzak" paints a comprehensive picture of the U.S. Army Signal Corps transitioning into the modern era – a time when technology rapidly altered the character of war. Parker Hitt is a highly relevant tale for today's professionals as the Army once again finds itself on the precipice of major technological changes that will redefine modern warfare.

Parker Hitt in an undated picture as a colonel in the Army. (Courtesy image)

Author

Ivan Zasimczuk graduated from the University of California at Davis (UCD) with a Bachelor of Arts in History and Political Science, and a minor in English. He joined the Army through the UCD Reserve Officers' Training Corps and entered active duty in 1997 as an adjutant general officer. Zasimczuk has served in Germany, Bosnia, Kosovo, Kuwait, Iraq, and Jordan. He attended Kansas State University earning a Master of Arts in History with a follow-on teaching assignment at the United States Military Academy at West Point where he taught Military History and Leadership. He retired in 2017, then worked at the British Embassy in Washington D.C. for one year Zasimczuk currently works at the U.S. Army Signal School. He is a frequent contributor to Army History Magazine.

From Crisis to Capability: The Evolution of Hermes

Soldier-led innovations

Master Sgt. Chad Johnson and
Capt. Christopher Pauley
U.S. Army Signal School

When the Army's Digital Training Management System (DTMS) experienced extended outages and performance limitations, organizations across the force were forced to confront a hard reality: Mission readiness could not pause simply because legacy systems became unavailable.

At the U.S. Army Signal School within the U.S. Army Cyber Center of Excellence (CCoE), leadership recognized the immediate operational impact these outages had on training management, personnel accountability, reporting accuracy, and organizational readiness. Rather than wait for a solution from outside the organization, an internal effort emerged to bridge the gap. That effort became Hermes.

Hermes originally began as a SharePoint-based application built using Microsoft Power BI and Power Apps. Developed to rapidly restore operational visibility during DTMS outages, the platform provided leaders with a centralized solution for tracking personnel, classes, readiness metrics, and organizational data in near real time. What started as a practical workaround quickly evolved into a critical operational capability.

The original version of Hermes focused on solving immediate readiness and management challenges through:

- Centralized training and personnel tracking
- Real-time accountability
- Course and class management
- Barracks utilization visibility
- Instructor and student data synchronization
- Automated and improved reporting workflows
- Dashboard-driven leadership visibility through Power BI analytics

Because Hermes leveraged SharePoint architecture alongside Power Platform capabilities, the system was able to be developed rapidly while remaining flexible enough to adapt to constantly evolving operational requirements at the Signal School.

Success of the platform demonstrated the demand for agile, mission-focused software developed directly alongside operational users rather than relying exclusively on large-scale enterprise solutions.

As adoption expanded and requirements matured, Hermes evolved into Hermes 2.0 – a significantly more advanced platform developed collaboratively by Master Sgt. Chad Johnson and Capt. Christopher Pauley. Unlike the original SharePoint-based architecture, Hermes 2.0 was designed and built directly within the Army's Vantage environment, leveraging live enterprise data to create a dynamic operational ecosystem capable of supporting leaders in real time. The platform moved beyond traditional data management and became a fully integrated operational framework.

Hermes 2.0 logo created by Master Sgt. Chad Johnson, U.S. Army Signal School.

Built as a web-based Operational Software Development Kit (OSDK), Hermes 2.0 introduced:

- Live data integration through Army Vantage
- Real-time readiness dashboards
- Interactive personnel and course management
- Automated reporting workflows
- Barracks management and utilization tracking
- Training pipeline visualization
- Dynamic analytics and forecasting tools
- Enterprise-level accessibility through a centralized web architecture

The development team ultimately established the platform under its own dedicated domain: **hermes.vantage.army.mil**

This milestone represented more than technical growth; it reflected a shift in how operational problems could be solved from within the force itself. Hermes 2.0 demonstrated the effectiveness of pairing

operational experience with modern software development practices. By leveraging live data and building directly around user requirements, the platform significantly reduced administrative friction while improving leader visibility across multiple functional areas. More importantly, the project highlighted the growing importance of Soldier-led innovation. Rather than relying solely on externally developed enterprise tools, Hermes showed how operational units can rapidly prototype, develop, and deploy mission-focused capabilities that directly address readiness challenges in real-world environments. The collaboration between enlisted and officer leadership throughout the project also reinforced a critical principle within the Army modernization effort: **Innovation is most effective when technical expertise and operational experience are combined.**

As the Army continues to modernize its digital infrastructure and data environments, initiatives like Hermes provide a model for agile development, operational adaptability, and leader-driven transformation. What began as a response to a system outage ultimately became a proof of concept for the future of operational software development inside the Army. Hermes was not simply created to replace capability during a disruption; it evolved into a platform designed to redefine it.

Master Sgt. Chad Johnson serves as the Operations sergeant major for the U.S. Army Signal School He also leads the development of enterprise data solutions that modernize reporting, automate business processes, and provide senior leaders with data-driven decision support.

Johnson has served in key leadership positions including senior (Secure Mobile Anti-Jam Reliable Tactical Terminal (SMART-T) instructor/writer, and senior transmission systems operator/maintainer. He holds a Master of Science in cybersecurity and information assurance from Western Governors University and a Bachelor of Science in Music Production from Full Sail University. He has earned professional certifications including CISSP, CASP+, Security+, CySA+, and PenTest+.

Photo illustration of Master Sgt. Chad Johnson, left, and Capt. Christopher Pauley, bottom right. Some of the imagery incorporates AI-generated elements that were digitally enhanced, composited, and refined by the creator. (Created by Tài Doick, U.S. Army Signal School)

Capt. Christopher Pauley enlisted in the Army in August 2009, advancing to the rank of sergeant first class as a 25D (Cyber Network Defender) before receiving a direct commission to captain in April 2025 as a Data Systems Engineer (26B). He currently serves as the Chief Data Officer for the U.S. Army Signal School.

Pauley's previous key assignments include serving with the Army Software Factory's inaugural cohort as a platform engineer, where he architected cloud-based containerized platforms and CI/CD pipelines for application developers. He holds a bachelor's degree in cybersecurity and information assurance from Western Governors University, complemented by numerous industry-level certifications in Kubernetes, cloud computing, and IT/cybersecurity.

Cyber Key Terrain for the Non-Technician

Theory talk

Lt. Col. Jerome M. Althoff
Advanced Civil Schooling, University of Denver

In this article, I combine my love of history and teaching. I attempt to take some technically challenging theory and provide concepts that make the theory more approachable to individuals in disciplines not involving signal or cyber. The goal is to reduce the perceived complexity of pure cybersecurity and offer alternative ways to understand some of its fundamental terms and mindsets.

This article aims to make the concept of key terrain in cyber operations more approachable to non-technical readers. Granted, defining cyber could easily spin off into its own series. Here, it will be used as a colloquial term encompassing technologies and methods used in modern digital communication, commerce, and warfare. This is important to both those who work within the Cyber branch and everyone else, as it has become a domain of the modern world and its battlefield. Like many complex things, I will attempt to build abstractions to make discussion manageable. By building abstractions and using historical and non-technical examples, I aim to provide a clearer perspective.

The Joint Force explicitly defines three layers of cyberspace: physical network (things we can touch: wires, power, etc.), logical network (e.g. software, protocols), and cyber-persona (the "acting" element) (JP 3 -12). A helpful analogy might be American railroad terminology. Most people do not have specifics of railroads in their daily lives, yet they can likely dredge up some terms like "all aboard, dining or sleeper car." In the same vein, people generally pay little attention to the specifics of cyber, though they can appreciate that a firewall is somehow always the problem.

Moving forward, I will provide several mental constructs that should be useful as well as identify what I believe to be the most essential cyberspace key terrain features.

Layers: Physical Network, Logical Network, and Cyber-Persona

All aspects of warfighting have key terrain – many with significant overlap. While a logistician or a maneuver expert might recognize a town, bridge, or hill as key terrain for different reasons, the "thing" physically exists and can be fought over.

Some physical terrain provides greater advantages to either friendly forces or the adversary and enjoys the moniker "key." A hill overlooking a flat expanse of ground is a prime piece of key terrain – one we can all visualize and internalize. The topography, hydrology, and flora of that hill constitute overlays that aid in understanding what "the hill" is easier and more discrete, which influences how and where we fight. Just as the hills overlooking a small Pennsylvanian town were key terrain for the battle of Gettysburg – hills which gave Union forces a literal upper hand – that hill is a chunk of our physical world. It is physical key terrain.

But what about key terrain in cyberspace? Just as physical terrain has overlays of topography, hydrology, and fauna, cyber has its own overlays: the physical network, the logical network, and the cyber-persona.
Physical Network Layer

Cyberspace's physical overlay is loosely contained by two terms: transport and devices. Transport refers to all the methods in which memes move, including wireless (Wi-Fi, Bluetooth, near-field, infrared, etc.) and wired (fiber, copper, etc.). Devices cover all the various media that people use to see, edit, or create memes as well as the intermediary equipment required to spread memes. This is somewhat akin to railroad infrastructure with the train as the meme, rails the transport, and the various stations the devices. Generally, physical aspects of cyber infrastructure can be targeted in the same way as hills or bridges and can be planned for accordingly. It is eminently possible to target the physical fiber and copper lines, as well as the antenna and transceivers used for wireless.

Early morning Aug. 5, 1914, began with the British navy dispatching a ship to dredge up and cut the trans-Atlantic telegraph cables of the German Empire. This is the first example of severing global electronic communications.

With the transport split, Imperial Germany had no alternative electronic option but to send their messages via the infrastructure owned and operated by their British adversaries. This was possible largely due to geography. There were few ideal locations in Europe for the trans-Atlantic cables which made it easy for the key terrain to be decisively seized (Corera, 2017). The same routes that once carried telegraph lines across the Atlantic now host the intricate web of our modern global fiber optic cables. The routes that painstakingly began in a pre-American Civil War era are now widely known and even more vulnerable to sabotage.

Now for the invisible elephant in the room: the electromagnetic spectrum (EMS). It is our term for the incredible span of energy that surrounds us. Humans

have managed to tap into EMS, thus enabling wireless communications, since the late 1880s.

Over the subsequent 140 years, our ability to utilize the EMS has increased exponentially. This has led to streaming music from the cloud to your phone, then to your wireless headphones, all while you navigate a city using real-time location information updated by satellites. EMS is a massive enabler with myriad applications. It is also easily susceptible to interference from both natural and manmade, innocent and intentional actions.

In 2013, a team of student researchers from the University of Texas at Austin managed to GPS spoof an $80 million yacht. While the crew and passengers could see the ship changing course, the yacht's command and navigation system still displayed as though the ship was on its initial course (Austin, 2013). Just over a decade later, use of EMS is more prevalent, as are its associated risks. A review of current events in Eastern Europe should provide plenty to think about regarding EMS operations.

During World War II, another EMS-based command and control issue led to an instant strategic upset.

Maneuvering forces across time and space to strike decisive blows required humans in the loop during the 1940s. There were no autonomous drones or artificial intelligence (AI) driven weapon systems. But just as drones or AI need some initial guidance, the humans controlling aircraft and ships in the Pacific did, too. This was generally done via wireless telegraphy, restricted from the adversary by using cryptography.

U.S. Naval cryptanalysis was able to break the Japanese Imperial Navy's code and provide details on when and from where the attack on Midway would occur. Admiral Chester W. Nimitz was quoted as saying, "Well, you were off only five minutes, five degrees and five miles out" (Carlson, 2011), which in the Pacific gave Allied forces what they needed to stop the driving wind behind the Imperial Japanese forces. Once they lost their secure command and control, their forces' effectiveness was reduced, followed swiftly by the sailors, pilots, and ships.

Logical Network Layer

The logical overlay of cyber is much more abstract. How devices talk to each other, how memes are packaged and sent, how to ensure only the intended audience can enjoy the meme, and how content is transported from an initiator device to an intended device are all examples of how cyber operates in the logical realm. Consider a box filled with train parts in a child's playroom. Regardless of well-intentioned adult intervention and organization, the various sets commingle. Tracks, scenery, cargo, gauges, even forms of locomotive technology will be mashed together in multiple configurations – each existing for a period, each working to some degree – before being reimagined. This ever-changing reality resembles the hodgepodge nature of the logical overlay. New pieces of logic are continuously created, either out of nothing or by bringing existing pieces together. This requires constant vigilance over the logical overlay. Logically, the world truly is flat and can fit in your pocket.

Cyber Key Terrain

Today, there are five states on the Iberian Peninsula: Spain, Portugal, France, Andorra, and the United Kingdom. In the 1150s, there were many more Christian kingdoms and Muslim emirates with shifting borders and allegiances. One particularly powerful king was Ibn Mardanīsh, known as "Wolf King." He carved out his kingdom as the Almoravid Emirate fell to the Almohad Caliphate. Over time, Wolf King aligned with other regional powers to continue to secure his realm. With extensive and organized kingdoms boxing him in on his north and west, Wolf King's primary source of growth was to the south and east. These regions were suffering disorder and fragmentation during the transition from Almoravid to Almohad authorities. Wolf King chose to besiege Cordoba in 1159. City leaders did not think they would outlast Wolf King, so they asked for help from the city of Seville. Leadership in Seville came up with a plan: an agent posing as an oil merchant sent by a fake noble of Seville.

Seville was both a significantly more attractive city-state to capture and much better prepared to withstand a siege – unless, of course, the city could be delivered to Wolf King. The agent went to Wolf King's court and convinced him to break the siege and move to Seville. Because he believed this messenger, he failed to take either city (Kennedy, 2014) (Eastaugh, 2023).

What relevance does cyber have to a military campaign conducted 865 years ago? Decisions ultimately stem from trust, trust comes from being able to identify the players on the battlefield, and in JP 3-12, that is wrapped up in cyber-persona. This aspect of cyber key terrain is the single most important, being essential to all permutations and combinations of any consideration of cyber key terrain. Without a solid understanding and control of cyber-persona within your mission planning, all other key terrain and the ability to command troops outside of shouting range is mute.

Validating who you are, who the other person is, and maintaining that validation is paramount. By this point, most people are likely being irritated by the increased use of multi-factor authentication, even if they know deep down it is essential. Authentication apps, physical keys, push notices, one-time pins, and phone calls are all examples of increased focus on validating identity. Just as Wolf King learned, if you trust the identity of someone or something without

verification, you can lose out on acquiring your next city-state, access to your banking, or control over your maneuver elements. Clicking on a link, opening an email, or accepting position location information – someone's location on the planet - are all actions that need to happen so we can do our jobs. All of that relies on you being you, them being them, and both knowing it.

The National Institute of Standards and Technology recommends separating duties as a security procedure. One way that organizations accomplish separation of duties is to have multiple accounts and account types (Vincent Hu, 2017). Separation of duties reduces the risk of insider threats and error while increasing the chance of discovering fraud.

One effective method that organizations use to implement separation of duties is to provision multiple user accounts and account types for different roles and tasks. This ensures that no single individual controls all critical functions of a process, thereby enhancing security and compliance.

Everyone is likely familiar with the terms user and administrator. Just as a point of interest, any account that is not directly related back to a person falls under the umbrella of non-personal entity – covers things you might have heard of like service or system – are mostly used on the system backside to accomplish a wide range of repetitive or known actions and used to distinguish them from human action. They are generally easier to secure and monitor as they complete their designated tasks. Any action performed outside of their normal activities would ideally raise an alarm. Ensuring that these accounts are secure and performing only their designated functions is an essential aspect of the cyber-persona key terrain.

Focusing on both strengths and weaknesses of the cyber domain, we can concentrate on the common human accounts – user and administrator. Each one of us is a user, and most of us are also administrators on our own devices. What is the difference between the two and how do we know which identity to interact with? A user can only interact with something in a defined way: play the game, enter the data, join the meeting, etc. Administrators can modify the conditions, means, allowable inputs, and destinations of outputs. Typically, hackers are users who are attempting to gain unauthorized administrative privileges or perform unintended actions, which exemplify a user exceeding their assigned identity.

A simple analogy: You are always you, but the clothes you put on changes how you represent yourself and how others perceive you. If you wear a red, orange, or blue shirt at a big box store, you should be prepared to answer questions, as you may be causing identity confusion.

With a basic understanding of the difference between user and administrator being analogous to a change in outfits, and further with the rapid ability to "look" the part based on easy changes to appearance, the driving imperative to know who one is hopefully makes more sense.

Knowing who someone is increases the ability to secure the environment by time, location, role, function, or some combination of things. Being able to positively identify the individual and tie their actions, user or administrator, is fundamental to them. Many failures of cybersecurity are caused by failures surrounding identities.

As AI-related technologies continue to blur lines of human and machine, we have seen machines pass the Turing test, both verbally and written.

Deepfake or deceptive visuals (still or motion) render our eyes suspect. Coupled with the ability for AI to mimic a human's voice and emotional nuance with only seconds of audio from the individual, we now must question our ears (Edwards, 2023). We could be left wondering which orders do we follow, which is the voice of the commander, do we flank, charge, or withdraw? We will continue to wonder that if we lose control of the cyber-persona – the single most important piece of cyber key terrain.

Take Away

Cyber is a strategic fight that can last a few minutes or span multiple years. While its physical aspects (devices, wires, antenna) are easy to see and target, the electromagnetic and logical portions are impossible to see with the Mark1 eyeball.

It takes education, analogies, and determination from all personnel – uniformed and civilian, entry-level through senior leadership – to understand and fully appreciate the dangers that come hand-in-hand with all the daily benefits.

In addition to our collective military elements, it takes an educated population with their own personal resilience and understanding so they can better handle what will be needed to weather a large-scale, cyber-involved conflict.

References

Austin, U. o. (2013, July 29). *UT Austin Researchers Successfully Spoof an $80 million Yacht at Sea*. Retrieved from The University of Texas at Austin: https://news.utexas.edu/2013/07/29/ut-austin-researchers-successfully-spoof-an-80-million-yacht-at-sea/

Carlson, E. (2011). *Joe Rochefort's War: The Odyssey of the Codebreaker Who Outwitted Yamamoto at Midway.* Annapolis: Naval Institute Press.

Corera, G. (2017, December 15). *How Britain pioneered cable-cutting in World War One*. Retrieved from BBC News: https://www.bbc.co.uk/news/world-europe-42367551

Eastaugh, S. (2023, November 10). *Reconquista*. Retrieved from PodBean: https://reconquista.podbean.com episode-77-setbacks-all-around/

Edwards, B. (2023, 1 9). *Microsoft's new AI can simulate anyone's voice with 3 seconds of audio*. Retrieved from ars Technica: https://arstechnica.com/information-technology/2023/01/microsofts-new-ai-can-simulate-anyones-voice-with-3-seconds-of-audio/

Kennedy, H. (2014). Muslim Spain and Portugal. Routledge eBooks.

Vincent Hu, R. K. (2017, June). *Verification and test methods for access control policiesmodels.* Retrieved from NIST: https://csrc.nist.gov/pubs/sp/800/192/final

Author

Lt. Col. Jerome M. Althoff is a functional area officer (information network engineer/26B). He was an infantry officer with 2nd Cavalry Regiment, then a signal officer at the 101st Airborne Division (Air Assault),173rd Airborne Brigade, National Ground Intelligence Center, and U.S. Army Training and Doctrine Command G6. Althoff's passion for enabling communication, education, and amateur study of history come together to help bridge the gap from the depth of the Signal Corps to other warfighting functions.

The Enduring Signaleer: Building a Resilient Network Through People and Data

It begins with people

Chief Warrant Officer 4 Gairie M. High
U.S. Army Signal School

When most people think about a network, they often picture technology: radios, computer and storage platforms, cables, satellites, cloud environments, and countless systems that enable information to move across battlefields and around the globe. As the Army continues to modernize, these technologies are becoming increasingly interconnected and diverse across the force, creating new opportunities – as well as new challenges – for those responsible for integrating, operating, and sustaining them. While the equipment may evolve, the true strength of our network has always been its people.

For generations, Signal warrant officers have served as the Army's trusted technical experts, operating at the intersection of technology and mission execution. As new capabilities emerge and the operational environment becomes increasingly complex, no sole warrant officer can be an expert in every system or technology fielded across the force. The enduring strength of our cohort lies in our ability to leverage the collective expertise of fellow warrant officers to solve problems and accomplish the mission.

Strength of the Cohort

The Signal Warrant Officer Cohort serves as the connective tissue that binds the Army's technical community together. Whether enabling data centric operations, managing complex networks, or defending the Army's digital terrain, warrant officers routinely leverage the collective expertise of their peers to solve problems, close capability gaps, and deliver operational outcomes.

This culture of collaboration and knowledge sharing remains one of the greatest strengths of our profession. As the Army continues to modernize, the ability to rapidly identify expertise, share lessons learned, and connect technical professionals across the force will become increasingly important. The resilience of our network is not found solely in the technologies we employ, but in the relationships and expertise that enable us to adapt, innovate, and overcome challenges together.

Preparing the Next Generation

At the U.S. Army Signal School, we intentionally expose students to this reality early in their development. While technical proficiency remains essential, we also want future warrant officers to understand the value of the professional network that exists across the force. The relationships being built today and the connections established throughout careers often become the difference between spending days problem solving alone and resolving a problem with a single conversation from someone who has already faced a similar challenge.

Leveraging Data to Strengthen Connections

To help reinforce this concept, students are leveraging enterprise data platforms – such as Vantage – to aggregate, analyze, and visualize information about the warrant officer cohort.

Through use of modern data tools such as Power BI, they learn how to transform raw data into meaningful visualizations that provide greater visibility of the warrant officer population. By connecting data from multiple sources, students gain a better understanding of the cohort and learn how data can be used to identify trends, close information gaps, and support better decision making.

More importantly, these visualizations help students connect the dots across the Army. They provide visibility of warrant officers serving across the globe, allowing students to identify individuals whose experiences, technical expertise, and operational backgrounds can help them solve problems and overcome challenges. In many ways, these efforts mirror the very thing that has always made the Signal Warrant Officer Cohort successful: connecting people with knowledge to people who need it.

By leveraging enterprise data through platforms such as Vantage and visualizing it through Power BI, we are making those connections more visible and accessible to the next generation. We are not simply creating visualizations; we are revealing connections that already exist.

The Enduring Signaleer

The enduring Signaleer understands the Army's most valuable network is not defined by hardware, software, or infrastructure. It is defined by the people who sustain it.

By leveraging data to better connect expertise across the force, today's Signal warrant officers are

ensuring that the next generation is prepared to adapt, innovate, and solve the challenges of tomorrow. In the end, the strength of our network is measured not only by the technology we field, but by the people who stand behind it.

Author

Chief Warrant Officer 4 Gairie M. High enlisted in the Army as an information systems operator-analyst (74B) in 2004. He was appointed as a warrant officer one in 2012. Upon graduation from the Warrant Officer Basic Course, was awarded the 255A military occupational specialty (information systems technician). High currently serves as the senior technical advisor for the Warrant Officer Branch at the U.S. Army Signal School, Fort Gordon, Georgia.

Road Show Initiative Bridges Change, Builds Buy-in

IT overhaul

Article, photo by Candy Knight
2nd Theater Signal Brigade Public Affairs

The 39th Strategic Signal Battalion (SSB) launched a Road Show initiative, central to 2nd Theater Signal Brigade's (TSB) Network Enterprise Centers Consolidation project, to drive workforce communication and engagement amid organizational change.

The Road Show was born out of the NEC Consolidation effort to address the sweeping changes impacting Soldiers and Department of the Army civilians as key IT functions are centralized. The initiative was coordinated by Lt. Col. Ryan G. Tintera, executive officer, 39th SSB.

"Our Soldiers and civilians are facing new roles, increased automation, and shifting responsibilities as we reduce our NECs from four to two: NEC Benelux and NEC Poland," Tintera said. "The Road Show is our way of clarifying these changes, answering questions, and fostering buy-in across the battalion."

One of the goals of the Road Show is to improve integration between Soldiers and Department of the Army civilians. The battalion created a hybrid NEC structure where Soldiers are paired with civilian partners based on their military occupational specialty, such as Enterprise Services or Network Services.

Leadership believes Soldiers and civilians can learn from each other through these partnerships. Additionally, the newly established 'Watchdog Academy' offers in-house training for standard civilian IT certificates to both Soldiers and civilians. Tintera also noted that past reorganizations highlighted the need for more workforce input.

The 39th SBB launched a Road Show initiative, central to the 2nd TSB's Network Enterprise Centers Consolidation project, to drive workforce communication and engagement amid organizational change.

"This time, we led the Road Show with the executive officer, NEC director, and S3 to create a comfortable environment where Soldiers and civilians could voice concerns and share feedback," he said.

As the Army adapts to changing resources, it is using automation to streamline operations and training Soldiers to take on responsibilities that were previously managed by civilian staff.

During the Road Show, leaders demonstrated new technologies, such as Azure Virtual Devices and Commercial Solutions for Classified, that enable Army personnel stationed at geographically isolated locations and at NATO partner installations to securely connect to Army networks and use essential IT resources without needing on-site technical support.

To address questions from employees at different locations about supervision and guidance, leadership will conduct more virtual meetings, publish clearer guidance, and visit sites to stay connected to key stakeholders.

"You cannot mandate transformation; you have to build genuine buy-in from the ground up," said Nichoals Carbone, deputy commander, 2nd TSB. "Civilians and local nationals are the continuity of our force, making up a third of our team. It is absolutely essential that our Soldiers, civilians, and local nationals are fully aligned and working side-by-side. That shared understanding is the only way we can deliver the standardized, seamless services this consolidation aims to achieve."

Leadership continues to assess the needs of mission partners and adjust organizational plans to ensure the battalion remains responsive and effective.

The Road Show team visited every site, emphasizing a collaborative approach that fostered candid feedback and strengthened relationships across the battalion as it continues its modernization efforts.

"Transformation only succeeds when our people understand the mission, see their place in it, and have a voice in the process," said Col. Slade Smith, 2nd TSB commander. "The Road Show helps build trust and improves collaboration between Soldiers and civilians. It also reinforces that modernization is not just about technology; it is about creating a more agile adaptive force to deliver reliable communications to the warfighter anywhere in the theater."

The Anchor and the Compass: Reflections on 40 Years of Service

'A profound privilege'

Dr. David L. Verret
U.S. Army Signal School

Forty years ago, I took an oath to support and defend the Constitution. My journey began as an Army air traffic controller, continued through service in U.S. Space Command, and eventually led to my current role as a civilian overseeing the Regional Signal Training Sites (RSTS) Division. Across four decades – through evolving technologies, shifting missions, and changing organizations – the principles that anchor a meaningful life and career have remained constant.

If these years have taught me anything, it is that leadership is not defined by rank, title, or resources. It is defined by character. The secular wisdom of self-mastery and the enduring truths of Holy Scripture have been woven throughout my journey, serving as both anchor and compass through every transition.

Private Victory: Stewardship and Intent

Leadership of others begins with leadership of self. Stephen Covey, Best-selling author and educator, described this as the "private victory" – taking responsibility for one's choices and being proactive rather than reactive. Scripture echoes the same principle: "Whatever you do, work at it with all your heart…" (Colossians 3:23). For me, this meant focusing on what I could influence instead of what I could not influence.

Beginning each mission and day with the end in mind helped align my actions with integrity and excellence. True discipline lies in putting first things first and choosing importance over urgency.

Public Victory: Humility and Collaboration

Service becomes truly impactful when we shift from independence to interdependence. While directive leadership is common in military environments, lasting influence comes from seeking "win-win" outcomes grounded in an abundance mindset. This principle guided my stewardship of a $10 million annual budget and a combined workforce of government civilians and contractors across multiple Regional Signal Training Sites.

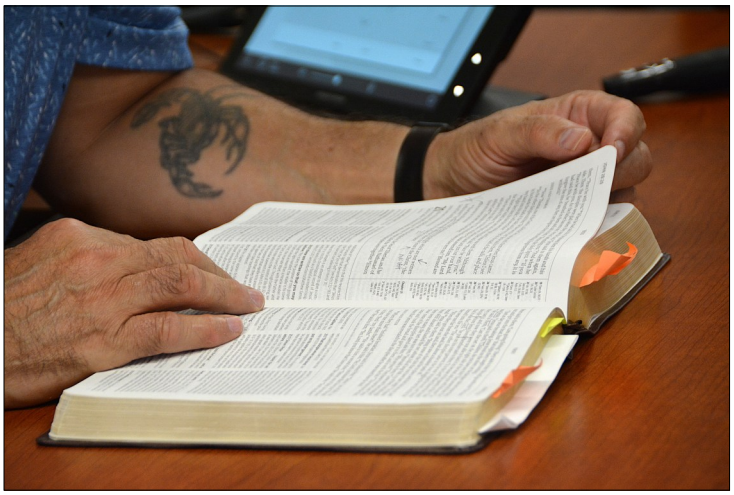
Effective stewardship demands humility, deliberate communication, and a commitment to shared success. It requires seeking first to understand, then to be understood – echoing James 1:19: "Be quick to listen, slow to speak…" From empathy and trust grows synergy, where the collective strengths of a team produce results no individual could achieve alone.

Continuous Renewal: Sharpening the Saw

Enduring four decades of service requires continuous renewal across four dimensions:

- **Physically**: Maintaining discipline and energy.
- **Mentally**: Pursuing rigorous academic growth, earning my doctorate, teaching graduate-level computer science as an adjunct professor for several universities, and continuing advanced study as proof that intellectual renewal never stops.
- **Socially and Emotionally**: Investing in your family, community, and colleagues.
- **Spiritually**: Grounding your daily life in prayer and reflection, remembering Isaiah 40:31.

Dr. David L. Verret is honored for 40 years of federal service during the U.S. Army Cyber Center of Excellence Town Hall at Fort Gordon on May 29, 2026. (Photo by Spc. Samantha Powers, U.S. Army Cyber Center of Excellence)



Dr. David L. Verret largely credits "Holy Scripture" with his successful 40 years of federal service. (Photo by Laura Levering, U.S. Army Signal School)

A Legacy of Service

Legacy is ultimately measured in people. I am most proud of the Soldiers, civilians, and contractors I have had the privilege to mentor – individuals who have gone on to lead, teach, innovate, and serve with distinction. Their success remains the greatest reward of my career.

To those who follow, alignment precedes assignment. Lead with values before position. Guard your character as closely as your credentials. Choose wisdom over recognition and responsibility over visibility. Leadership is a temporary stewardship of trust. Forty years of service has been a profound privilege. The mission continues, and I remain grateful for every challenge, opportunity, and person who shaped this journey.

Author

Dr. David Verret currently serves as Chief of Regional Signal Training Sites and Signal Mobile Advanced Readiness Training. His career includes multiple combat-era deployments to Kuwait and Afghanistan in key G6 and S6 leadership roles. Dr. Verret holds a Doctor of Science in information systems and communications from Robert Morris University, complemented by advanced degrees in information technology management and electronic systems technologies. A published author and adjunct professor, he is a recognized authority on capability development and end-user experience in military communication systems.

Impacts of C2 in Degraded Network Environments

Topologies

Article, graphs by Lt. Col. Clifton Russ
Joint Enabling Capabilities Command

As a second lieutenant, I attended the Signal Officer Basic Course (SOBC) not knowing what to expect. Most notably, I remember being handed large printouts of the Mobile Subscriber Equipment (MSE) to study while simultaneously being told that we would never see this equipment in the field.

Although the Army had already transitioned to the Joint Network Node (JNN), the curriculum had not caught up. During this time, the U.S. Army Signal School focused on providing "voice to the warfighter" in tactical environments in support of brigade combat teams (BCT). There was little to no discussion on the cybersecurity aspects of our roles. Signal Captains Career Course was marginally better. It wasn't until I returned for the functional area Automations Officer Course (now 26B, Data Systems Engineer) where cybersecurity had a strong presence in our curriculum. This knowledge provided opportunities to build and maintain a resilient network.

Given our role of ensuring voice to the warfighter, how can Signaleers support the command and control (C2) of an organization? Joint Publication (JP) 1 defines C2 as the "exercise of authority and direction by a properly designated commander over assigned and attached forces" (JP 1, Doctrine for the Armed Forces of the United States, n.d.). Commanders' abilities to make timely decisions allow them to disrupt the adversary's decision-making and execution cycle.

Quick and efficient decision-making allows the commander to gain an advantage through executing a high tempo of operations (*JP 1, Doctrine for the Armed Forces of the United States*, n.d.). Whether it's MSE, JNN, Warfighter Information Network-Tactical (WIN-T) or Integrated Tactical Network (ITN), how can Signaleers enforce resilient networks for command decisions?

Topologies

It is probably unlikely for a signal officer to arrive at an organization with the resources to fundamentally alter its communication architecture, but it is important to understand security options that we have at our disposal. One approach that we can do is to better understand network topologies, specifically centralized and distributed (or decentralized).

Centralized topologies include individual nodes connected to a central server that consolidates all of the information received from nodes. The server acts as a hub, enabling nodes to share resources by relaying information to it (Xi, 2020).

Primary advantages of centralized topologies include storing, locating, and managing information, such as using file directories. However, this simplicity makes the network more susceptible to adversarial attacks. Contrarily, distributed networks do not have a central server. Instead, nodes in decentralized networks act independently of each other (Xi, 2020).

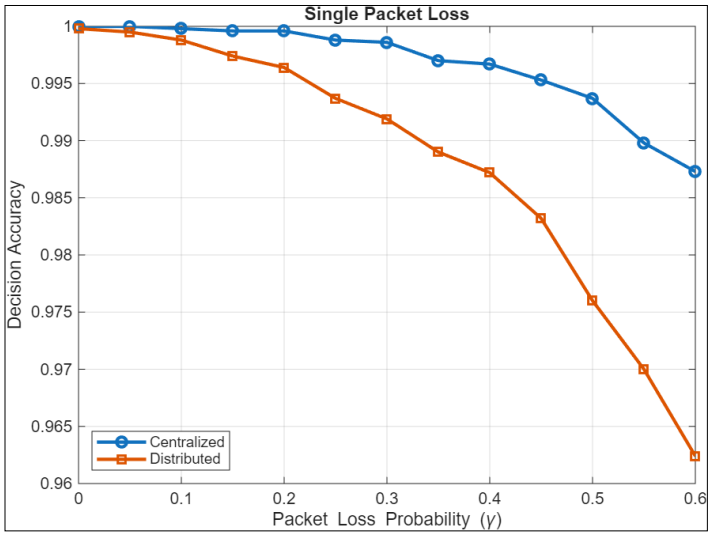
Historically, society operated with centralized networks until internet use increased. The internet is designed to operate in a decentralized topology, where data is routed from one node to another without requiring knowledge of all nodes (Lucky, 2017). Since then, internet applications such as social networking and streaming platforms have pushed a need for cloud computing. These Software-as-a-Service (SaaS) platforms and other cloud services recreated the need for centralization. Increased customer demand led to greater reliability in cloud services.

While cloud services reduced the need for physical infrastructure (also reducing costs), they also created single points of failure. The failure of a particular application could not only cause significant harm, but provide legal concerns, privacy concerns, and a lack of control. These concerns led to the movement to decentralized cloud infrastructures (Balangu, 2022)

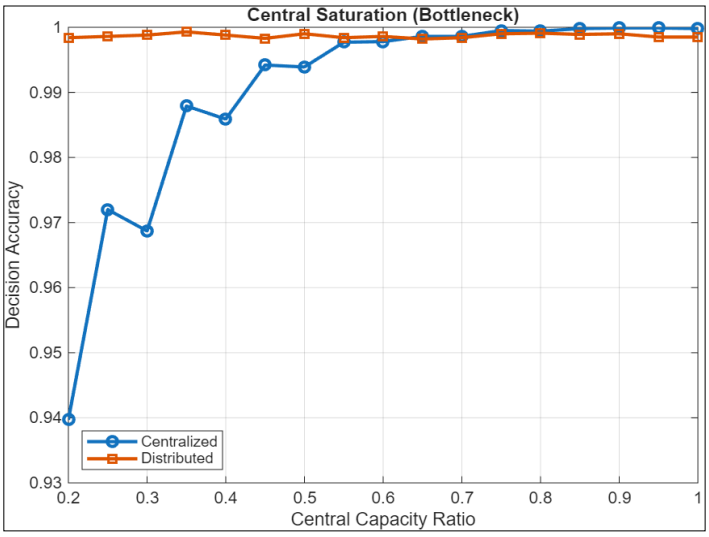
Signaleers must understand their organization before promoting a particular topology. It's easy to focus on the "new shiny object" or operate within our comfort levels. However, not only do the wrong topologies come at a monetary cost, but they might also impact our fundamental ability to give voice to the warfighter. As part of this research, I conducted simple simulations of degraded centralized and decentralized topologies to measure the C2 efficacy of an organization.

Methodology

The coding program simulates leadership decision making in six scenarios for centralized and decentralized networks. In both topologies, the commanders' accuracy is measured by the commander's decision accurately depicting the ground truth. In other words, does the commander have sufficient information to make a decision? For instance, suppose you are setting up a video teleconference (VTC). How much network degradation can exist for the commander to receive the appropriate information to make a decision? While



This graph depicts decision accuracy as the probability of a single packet loss increases. Both topologies begin with similar accuracies, but centralized topologies outperform the distributed topology as the packet loss probability increases.



This graph shows the decision accuracy as the available capacity increases. Since distributive networks have multiple routes, decentralized topologies outperform centralized topologies during a "Bottleneck."

this is an overly simple representation of "mission success," this simulation is a step to measure the impacts of degraded topologies. Each simulated scenario provides a different restriction that degrades the ground truth: independent packet loss, group node failure, a bottleneck, network isolation, bandwidth, and latency.

Independent packet loss determines the probability of an individual node dropping a packet for reasons such as interference or a link failure.

Group node failure examines the probability of a cluster of nodes failing, representing potential adversarial attacks, power failures or router issues.

A ***bottleneck*** represents a saturation of input at a local point, where there is more input than capacity, simulating potential memory issues or overflow.

Isolation of networks can either be intentional (split operations) or unexpected (physical damage).

Bandwidth deals with the probability of data loss as the data size increases which mirrors network congestion.

Latency references to a specific amount of data before an action occurs such as timeout thresholds.

Topology nodes represent the physical information technology (IT) network (sensors) and the social construction (units) of a centralized and decentralized network, depending on the scenario. This means a node can be the organization, e.g., battalion, or the physical link, e.g., Command Post Node (CPN).

In a centralized network, commanders wait for all information from subunits before deciding an action. In a decentralized network, commanders make decisions based off subunits actions. Both topologies undergo Monte Carlo simulations to measure commanders' impact. A Monte Carlo simulation is a technique of running a scenario several times with random samplings from a range of input (Harrison et al., 2010). Each scenario runs Monte Carlo simulations of the aforementioned restriction variables. After running each scenario, the program calculates the accuracy of the commanders making a decision.

Results

Key factors in the results include the number of nodes, sensing error rate, and the decentralization topology (ring, mesh, or full, and the number of neighbors). When the number of nodes reach 20, the accuracy between the two topologies is within ±2% accuracy difference. At 25 nodes, the difference is less than 1%, with an accuracy score of 99%. This means that there is correlation between the number of nodes and accuracy. The accuracy scores increase as the network nodes increase.

Lastly, commanders can maintain a 75% to 85% accuracy with a sensor error rate up to 40%. This means that the sensors can be incorrect up to 40% and commanders can have a decent accuracy rate. When the sensor error rate is above 50%, simulating a fully contested environment, decentralization outperforms centralization, but with low accuracy rates of 30 to 40%.

Generally, decentralization performs better for bottlenecks and latency. From an IT network infrastructure perspective, decentralization doesn't have a single point where a bottleneck can happen. From a communication perspective, the commander doesn't require all the data to make an informed decision. Similarly, delayed data negatively impacts commanders' ability to make timely decisions in a centralized topology.

Decentralization allows neighbors to continue to process information if one node is delayed.

Lastly, the decentralization composition played a significant role. Decentralized networks internally performed better as the number of neighbors per node increases. A simple ring topology does not perform as well as a mesh or a fully mesh network.

Closing

This simple simulation demonstrates how topologies can impact a network's efficacy. Although it requires more in-depth analysis to solidify exact findings, this simulation is sufficient to demonstrate the impacts of network degradation on different network topologies.

As Signaleers, we might not have the authorities or resources to fundamentally change an organization's network, but we can still provide voice to the warfighters utilizing basic network concepts.

References

Balangu, R. (2022, February 23). *The Evolultion of Decentralized Cloud*.

Harrison, R. L., Granja, C., & Leroy, C. (2010). *Introduction to Monte Carlo Simulation*. 17–21. https://doi.org/10.1063/1.3295638

JP 1, Doctrine for the Armed Forces of the United States. (n.d.).

Lucky, R. (2017, October 23). *The Lure of a Fully Decentralized Internet*.

Xi, Z. (2020). The comparison of decentralized and centralized structure of network communication in different application fields. *Proceedings of the 2019 International Conference on Management Science and Industrial Economy (MSIE 2019)*. 2019 International Conference on Management Science and Industrial Economy (MSIE 2019). https://doi.org/10.2991/msie-19.2020.10

Author

Lt. Col Clifton Russ is a joint planner at Joint Enabling Capabilities Command. Commissioned in 2006 through University of Memphis ROTC, he earned a Bachelor of Science in computer science with a double major in mathematics. Russ holds three Masters of Sciences and a Doctor of Philosophy in computational sciences and informatics from George Mason University. Russ has held key positions such as battalion and company command and the White House Communications Agency. Operational service includes deployments to Kuwait, Iraq and Afghanistan.

S6 Pioneering Air Defense Networks

Connecting the Shields

Capt. Brenden Jobe and Chief Warrant Officer 2 Nicola Sciara
1st Battalion, 51st Air Defense Artillery Regiment

The saying, "You can talk about us, but you can't talk without us," is a running joke in the Signal Corps that holds truth.
As you look across formations in the Army, you will find 25-series Soldiers enabling command and control (C2) from the company level to the corps level and beyond. The influence the Signal Corps has on the operational force cannot – and should not – be diminished to help desk tickets in garrison or setting up of OE-254 antennas during a command post exercise.

Every day, signal Soldiers are innovating and accomplishing missions to meet their commander's numerous lines of effort. One of the Signal Corps' core missions is to build resilient, reliable, and redundant C2 across Lower and Upper-TI capabilities for dispersed units.

The 1st Battalion, 51st Air Defense Artillery Regiment (1-51 ADA) is the first integrated fires protection capability (IFPC) battalion in the Army. The new IFPC equipment being fielded comes with the Integrated Battle Command System (IBCS) – a new fire control system – that uses the Integrated Fires Control Network (IFCN) to communicate from the Engagement Operations Center (EOC) to the weapons and sensors aligned to the unit. IBCS connects the sensors and effectors that were not originally designed to work together into one C2 system.

IBCS will enable a common connection capable system to an allow Army Air Missile Defense (AMD) such as Patriot or IFPC to communicate with Navy, Air Force, and Marine systems to enable a "best sensor to best shooter" concept. IBCS will enable any sensor and any shooter in the network to be connected and engage threats with any combination of systems available. This concept sounds effective, however, the current limitation for IBCS is that the IFCN network was designed to be line of sight (LOS) only. These systems have been in the design process since the early 2010s, and the battlefield has drastically changed during that time.

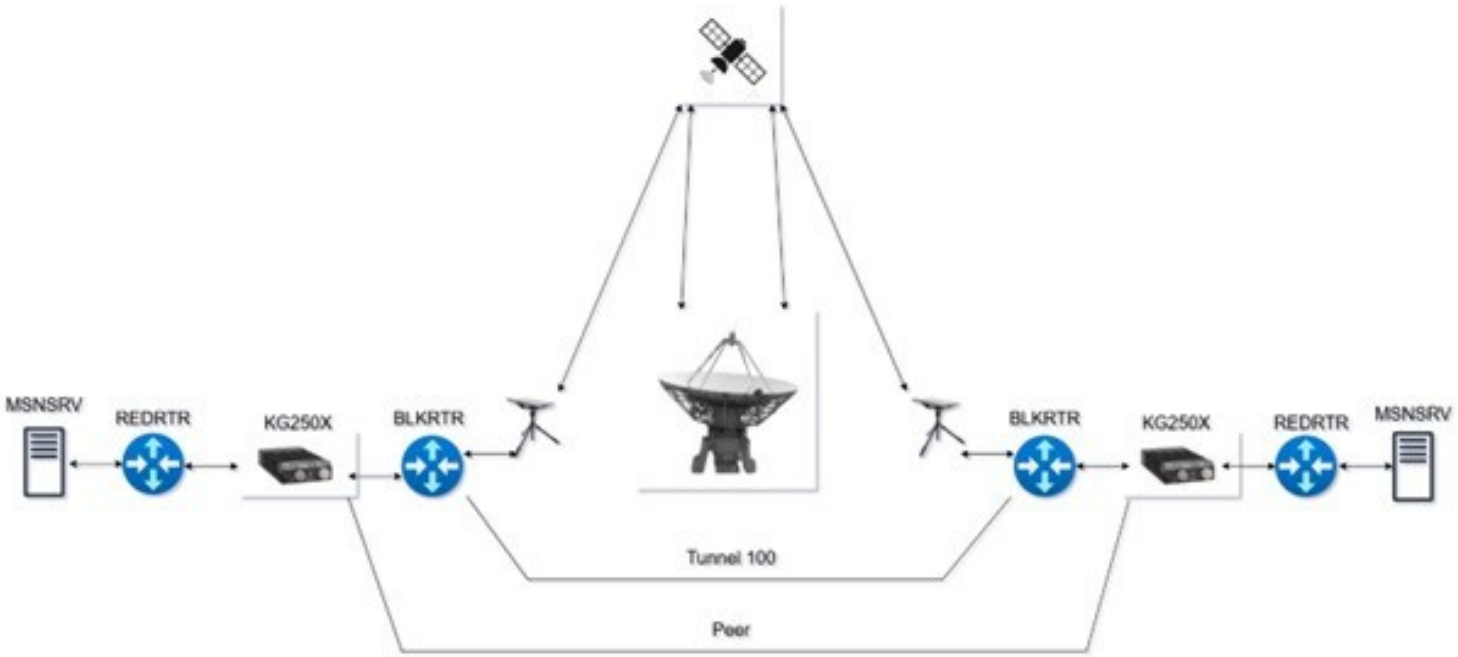
IBCS requires data through-puts per connection to pass target tracks and other pertinent data. During initial development, the only transports in the Army's arsenal to support this much data was LOS terminals such as high-capacity line-of-sight (HCLOS) to fulfill the data requirements. In the time that has passed since initial development, proliferated low Earth of 16-64 megabytes orbit (pLEO) has enabled the capability to turn this IBCS and IFCN into a beyond line-of-sight (BLOS) capable system.

IBCS utilizes Silvus StreamCaster 4480 tactical radios that have a normal LOS range of 40 km for ground-to-ground operations, depending on terrain and antenna configurations. The 1-51 ADA's mission is to provide protection to multi-domain teams (MDTs) within Multi-Domain Command-Pacific (MDC-PAC), such as the 1st Multi-Domain Effects Battalion (MDEB) and 5th Battalion, 3rd Field Artillery Long Range Fires Battalion (5-3 LRFB) in the first island chain in the Philippines.

Relying solely on these radios becomes difficult when the sensors, launchers, EOCs, and battalion fire direction control (FDC) are spread across the island of Luzon and possibly further south on other islands. This limitation becomes an impairment to the ADA mission to protect the force and critical geopolitical assets from missile strikes, aerial surveillance, rotary wing aircraft, and air breathing threats such as jet fighters or bombers. To overcome this limitation, 1-51 ADA tested a BLOS option by using Starshield and Internet Protocol Security (IPsec) tunnels to create connections to enable a battery EOC at Joint Base Lewis-McChord (JBLM), Washington, to connect to an MPQ-64A3 Sentinel Radar via IFCN Relay in the Philippines.

An additional asset belonging to 6th Battalion, 52nd Air Defense Artillery 6-52 ADA) at Osan Air Force Base, Korea, allowed their EOC to also connect to 1-51 ADA assets in the Philippines. On the Blackside router, an IPsec tunnel was established using AES -256 bit encryption with the tunnel source being the public IP of the Starshield locally at the EOC or IFCN Relay.

To make the connection work, it required the public IP instead of the carrier-grade NAT (CGNAT) that an end user normally receives from the terminal when someone directly connects. Once this was established, the KG-250Xs' on each side had connectivity to each other on the ciper text (CT) and plain test (PT) side, which allowed the redside router to learn routies through routing protocol protocols (RIP). Meticulous care must be taken when it comes to crypto statements for the tunnel configuration on the Blackside and proper communications security (COMSEC) keys in the KG-250X for proper transmission security (TRANSEC) to fully enable this capability.



IBCS Starshield Point-to-Point Network infographic. (Created by Chief Warrant Officer 2 Nicola Sciara, 1-51 ADA)

Using Starshield allowed for ease of use for the 14-series Soldiers in 1-51 ADA who have limited communications experience. Starshield also allows for ease of transport and is highly resilient. This allows for smaller teams, less technical expertise, and less of a footprint to establish a connection when compared to conventional means such as using an SNN with a Hawkeye III and 25-series Soldiers to man the equipment.

The Starshields are inherently robust dealing with adverse weather and other environmental factors, which was a huge positive for Soldiers operating in the Philippines where daily temperatures are typically in the high 90s with 80%-plus humidity. This connection established a single point-to-point connection which allowed radar data to be passed from the IFCN Relay in the Philippines to the EOC at JBLM with a latency of 300ms. This connection provided a BLOS solution to the IBCS/IFCN test equipment which has never been done before.

With 300ms latency, target quality (TQ) data was able to be passed from the Sentinel radar in the Philippines to the JBLM EOC almost 9,000 miles to allow for a remote engagement if necessary. The original design of the IFCN Relay and EOCs with the SILVUS StreamCaster radios would not allow for a proper connection to be established between the island chains or mountainous regions that make up the Philippines, let alone the BLOS connection from the Philippines to JBLM. 1-51 ADA was able to find this solution during Salakanib-Balikatan 2026 (SNBK26) by working with multiple air defense project managers, IBCS/IFCN field support engineers, and 6-52 ADA in Korea. We were able to test this setup from JBLM's EOC to the Philippines and then Korea's EOC to the Philippines to allow radar information exchange. Necessity is the mother of invention, and having all these teams come up with this solution allowed the concept of employment 1-51 ADA needs in the first island chain to become a reality.

In the ADA or FA environment, weapons and sensors need a dedicated BLOS capability that isn't throttled as it routed all over the Department of Defense Information Network. Additionally, normal LOS communications have limititations in mountainous regions or the islands of the U.S. Indo-Pacific Command area of responsibility (AOR). This limits each Air Missile Defense Task Force (AMD-TF) to the range of their IFCN. With the introduction of a BLOS capability, the AMD-TF can span the entire AOR instead of a smaller area size that 1-51 AD would be limited to – the first island chain being forced to use a LOS network. By using point-to-point or point-to-multipoint configurations that traverse the Starshield network, we can get over this hurdle.

1-51 ADA plans to keep pushing the limits of this BLOS capability by testing point-to-multipoint connection (EOC to 2-3 IFCN Relays) in Summer 2026 to build a mesh network in the coming year for future exercises with 6-52 ADA and other IBCS-enabled ADA battalions during SNBK27. This would enable a robust and capable network supporting the air defense shield for the first island chain.

Capt. Brenden Jobe enlisted in August 2015 as a cannon crewmember (13B) in the U.S. Army North Carolina National Guard before transitioning to the Simultaneous Membership Program, where he earned a Bachelor of History Secondary Education at Appalachian State University. He commissioned as a Signal Corps officer in 2020. Jobe currently serves as the S6 OIC at 1-51 ADA, MDC-PAC at JBLM. Washington. Jobe recently "completed the Joint Command, Control, Communications, Computers and Intelligence/Cyber Staff and Operations Course at National Defense University, Joint Forces Staff College, in Norfolk, Virginia.

Chief Warrant Officer 2 Nicola "Nick" Sciara is the network operations warrant officer at 1-51 ADA IFPC under the soon to be MDC-PAC. Prior to his time at 1-51, he was the network operations warrant officer at 2nd Brigade Combat Team, 10th Mountain Division, where he deployed to Iraq in support of Operation Inherent Resolve.

The NCO Induction: A Transitional Milestone

'Earned through adversity'

Command Sgt. Maj. Nathan B. Hunsaker
57th Expeditionary Signal Battalion-Enhanced

The transition from junior enlisted to the Noncommissioned Officer (NCO) Corps is a foundational milestone in a Soldier's career. Recently, Soldiers from 57th and 62nd Expeditionary Signal Battalions-Enhanced (ESB-E), 11th Corps Signal Brigade (CSB), proved they were ready to make that leap during a grueling, combined tactical NCO induction.

Departing from traditional garrison ceremonies, inductees were transported to a local training site to face an overnight crucible designed to test their physical endurance, leadership, and most importantly, their cognitive agility. Throughout the night, the future leaders navigated a gauntlet of physically and mentally demanding events. Training lanes included a High Mobility Multipurpose Wheeled Vehicle push, a rigorous functional fitness event, tactical casualty triage, a complex memory maze, a blind-lead communication exercise, and a Light Medium Tactical Vehicle load.

"Pain was temporary; the lessons were permanent," said Cpl. Eddie Brown, 57th ESB-E. "Today's induction reminded me that leadership isn't handed out with rank; it's earned through adversity."

The true test lay not in the physical weight of the tasks but in the ambiguity of the instructions. Evaluators provided each squad with intentionally vague guidance for each objective. The lack of step-by-step instructions forced the inductees to rely on each other, demanding that they communicate, collaborate, and think outside the box. The induction was designed to simulate the fog and friction of real-world operations, where leaders must assess a situation and develop an efficient solution on the fly.

"From specialist to corporal, the rank changed overnight, but the responsibility began long before the stripes," said Cpl. Jose Rodriguez, 57th ESB-E. "Leadership is no longer about being the best Soldier in the formation but about building those around you to be better."

The results spoke for themselves. Observers noted a stark contrast in how different teams approached the obstacles. Squads that took time to analyze the problem, formulate a plan, and leverage their collective intellect were able to execute operations with limited physical effort. By prioritizing mental agility and creative problem-solving over brute strength, these teams significantly reduced the friction of the challenges.

"No matter the hardships, no matter the cost, we push-forward – because the mission isn't optional; it's everything," said Cpl. Julia Palik, 57th ESB-E.

Ultimately, the combined induction served as a powerful reminder of what the modern Army requires of its junior leaders. While physical toughness remains a baseline requirement, the inductees demonstrated that the most effective weapon an NCO can wield is a sharp, adaptable mind.

"In today's fight, information moves at the speed of the conflict, and complex problems will be the normal for our junior leaders," said Command Sgt. Maj. Matthew A. Helmer, 11th CSB command sergeant major. "This tactical NCO induction took challenging situations and then enabled our inductees to think, create, and overcome problems that no one would see coming, much like the modern battlefield."

Soldiers from 57th and 62nd ESB-Es perform leader reaction tasks combined with chemical, biological, radiological, nuclear and explosives (CBRNE) training as part of a combined tactical NCO induction at Fort Hood, Texas. (Photo by Command Sgt. Maj. Maira McCoy, 62nd ESB-E)

Enforcing Commander-Defined Authority Windows in Tactical Networks

Hyunkeun Shin
Korea Research Institute for Defense Technology Planning and Advancement

Intelligence, Surveillance, and Reconnaissance (ISR) platforms tracked targets and transmitted data successfully in Ukraine. But by the time fire missions reached shooters, targets had already moved outside engagement envelopes (Gady & Kofman, 2024; TRADOC, 2024).

In Iraq, during Operation Iraqi Freedom, digitally transmitted targeting updates arrived after pilots had already acted on voice instructions (Ricks, 2006; GAO, 2006). In both cases, commanders did not default to voice radio because the digital network failed. They defaulted because they judged that digital data had already lost its right to influence the current action. These were not workarounds for a broken network. They were compensation for a network that succeeded at the wrong thing. The instinctive diagnosis is staleness: The data was old, so it was wrong. That diagnosis misses the structural problem.

"Commanders do not need a faster network. They need a network that knows when information has lost its right to influence the fight – and refuses to forward it."

Staleness is about age. This is about authorization**.** A three-second-old radar track is not simply "stale." It is no longer cleared for engagement because the commander's authorization window for that track has closed. A staleness problem is solved by transmitting faster. An authorization problem requires a mechanism that checks, before data enters the network pipeline, whether it is still valid for the current fight – regardless of how quickly it was delivered.

Every data type has a commander-defined window, or "action window," during which it remains authorized for operational action. Outside that window, data is not degraded; it is unauthorized. Military networks currently enforce no such boundary. Each successfully delivered packet is treated as cleared for use, regardless of whether that window has already closed.

The voice radio fallback illustrates exactly what is missing. A human operator judged that the digital information no longer had the right to influence the current action and refused to use it. That judgment was correct. The digital network had no equivalent structure. Time-Gated Transmission Architecture (TGTA) is the systematic replacement for that improvised human check. In a Joint All-Domain Command and Control (JADC2) environment where machine-speed systems act on incoming data without any temporal check, this gap does not merely degrade performance; it feeds stale targeting data into machine-speed decision loops before anyone can stop it. This article names that failure mode Structural Time Failure (STF) and proposes a fix: the TGTA.

Why Retransmission Mechanism Makes it Worse

Tactical networks are built on a reliability principle: If a message fails to get through, send it again. This design made sense when data volume was low and a human reviewed each message before acting on it.

In a high-frequency sensor environment – drones, electro-optical/infrared (EO/IR) arrays, ground robots generating continuous data streams – this resend-until-delivered approach creates a paradox.

In small-scale exercises with few terminals, this paradox remains latent. Collisions are rare, retransmissions limited, and most data arrives within its window. Failure only becomes visible when subscriber count surges, as it does at the onset of combat operations. By then, the system has already passed every test. Signal officers know this pattern: the network works in garrison, works in training, and fails precisely when it matters most.

Under network congestion, the retransmission queue fills with both fresh data and data the operation has already moved past. The network does not distinguish between them. Older messages, which have been waiting longest, often remain near the front of the retransmission queue and are forwarded first. The result is systematic inversion: the network preferentially delivers data that has already missed its window. This inversion worsens as network speed increases.

A faster network does not close the authorization gap – it accelerates delivery of data that was never cleared for the current engagement. The problem is not that data arrives slowly. It is that nothing checks whether data is still authorized before it is sent. Without that check, structural time failure is not a risk – it is a structural inevitability.

A 2022 NATO Command and Control Center of Excellence (C2COE) assessment of high-tempo ISR pipelines found that track data repeatedly arrived at command nodes after engagement windows had closed – while the network reported successful delivery throughout (NATO C2COE, 2022). Controlled simulation under wartime subscriber density confirms the scale of the gap: packet delivery remained above 82 percent while the Time-Valid Delivery Ratio for Class 3 traffic collapsed to zero. The network reported success. The operation had already failed (Shin, 2026).

Time as Authorization, Not Performance

The standard engineering view treats time as a performance variable to optimize. The argument here is different: time defines whether data still has a role in the current fight. Networks measure success through delivery rate, latency, and throughput. Commanders measure success by a single question: Did this information arrive in time to act on it? Colonel John Boyd's decision-cycle model captures the consequence: a force that cannot act on information within the relevant window loses the ability to influence the unfolding situation (Coram, 2002). Beyond that window, information may remain accurate and successfully delivered but it no longer has a role in the current decision.

Table 1 defines four Reaction Window classes, each representing the period during which a data type remains authorized for operational action. The classification does not assert that older information is worthless. Class 0 data retains its authorization indefinitely. It asserts that the authorization boundary for each class must be defined by commanders and enforced by the system. STF occurs when the system cannot distinguish between them.

Table 1. Reaction Window Classification by Data Type

Class	Authorization Window	Data Type	Cost When Unenforced
Class 0	No expiry — permanently authorized	Enemy doctrine, terrain overlays	None
Class 1	Hours	Route status, logistics data	Unauthorized route data delays resupply
Class 2	Minutes (30–60 min)	Troop positions, Close Air Support (CAS) coordination	Fratricide risk; missed engagement clearance
Class 3	Seconds (3–15 sec)	Radar tracks, time-sensitive targets	Fires on unauthorized track — mission failure

A Reaction Window is not a network parameter. It is a command decision defined by commanders based on the physics of the engagement and the speed of the threat. Adjusting it redefines who may authorize action on that information, in the same way that assigning fires clearance authority defines who may authorize lethal action.

Time-Gated Transmission Architecture

Existing approaches – Quality of Service (QoS) prioritization, deadline-aware scheduling, age-of-information metrics – each improve some aspects of timeliness. None acts on commander-defined windows; all three operate after data has already entered the pipeline. By then, data that has missed its window is competing for the same bandwidth as data still valid for the fight. The Reaction Window is set by commanders at mission planning, not computed from network conditions. The only point of prevention is before entry, and that is where TGTA acts.

TGTA enforces one rule at every relay point: before a message enters the pipeline, determine whether it will reach its destination while still within its authorization window. If yes, send it. If no, refuse it, and record that refusal for after-action review.

TGTA in Practice

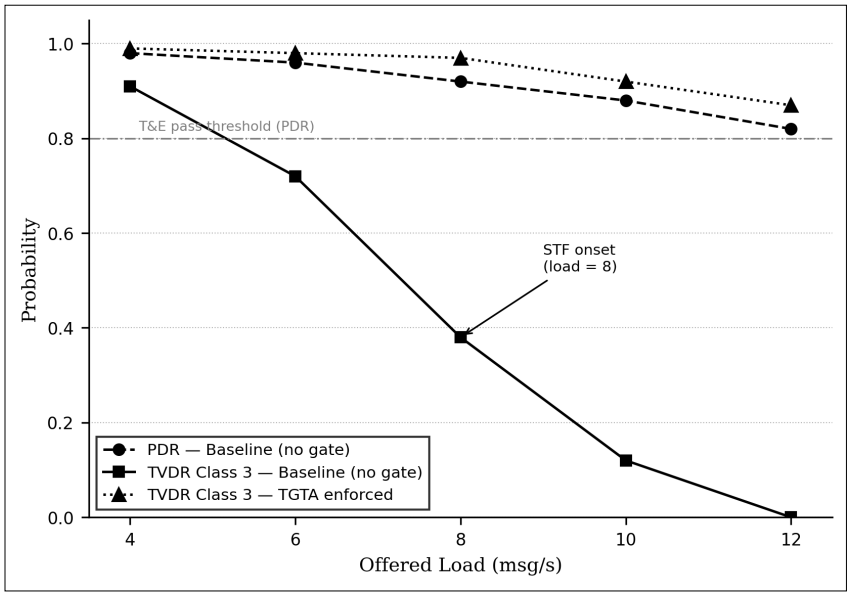
A radar track with a three-second authorization window travels through three relay nodes. At each relay, one question is asked: Will this track reach the C2 node while still cleared for engagement? If no – regardless of priority – it is refused, and the refusal is recorded. The fires cell never receives an unauthorized track. The commander's display shows only what is cleared for action. The network did not get faster; it became honest.

Authorization windows are assigned by commanders at mission planning – not derived by the network. TGTA is compatible with current Variable Message Format (VMF) and MIL-STD-2045 message structures

that can be fielded as an overlay on existing systems without hardware replacement (DoD, 2021). Systems without TGTA treat every delivered message as still valid for the current fight, regardless of when it was generated. That assumption is what produces STF.

Measuring What Matters: TVDR

The appropriate measure of operational success is the time-valid delivery ratio (TVDR): the percentage of messages that arrive while still within their authorization window.



Packet Delivery Ratio (PDR) vs. Time-Valid Delivery Ratio (TVDR) under increasing offered load, Class 3 traffic (3-15 seconds window). PDR remains above 65% while TVDR collapses to 4% without TGTA enforcement; TGTA restores time-valid delivery to 87%. Simulation: 3-hop chain, 80 kbps bottleneck, VMF message profile. (Chart generated by Hyunkeun Shin with Python/Matplotlib)

A network reporting 82% packet delivery and zero TVDR is efficiently certifying a system that delivers nothing operationally usable. Without TVDR, that failure is invisible – it never shows up in any standard network report, and the system passes every current T&E threshold.

Table 3 (below) shows what current testing misses: The same system that passes in a peacetime exercise delivers zero valid targeting data under wartime subscriber density. TGTA restored Class 3 TVDR to 87% under the same conditions without hardware changes (Shin, 2026). Every refusal is recorded, creating an after-action record that makes STF measurable for the first time. Table 3 summarizes simulation results at critical load.

Implications for Acquisition, Testing, Doctrine

Treating time as an authorization boundary rather than a performance variable has direct consequences for how systems are specified, tested, and commanded. Three actions follow.

Acquisition Specifications

Signal officers writing acquisition requirements today have a straightforward addition to make: configurable authorization windows and TVDR thresholds by message class, as mandatory functional items in any future tactical network request for proposal (RFP). Requirement documents without this language will produce systems that treat every delivered packet as cleared for use, encoding this gap into the force for a generation.

A 2025 Government Accountability Office (GAO) assessment found JADC2 data-sharing integration still operating at the "swivel-chair" level (GAO, 2025); TVDR is the metric that finally makes that integration measurable in operational terms.

Operational Testing

Signal officers and testers running JADC2 operational assessments need one additional line in their test criteria: TVDR alongside packet delivery ratio (PDR). A system that passes PDR thresholds while failing TVDR is moving data that has missed its window to commanders at machine speed and recording it as success. Combined exercises with partner forces should include deliberate TVDR measurement in sensor-to-shooter scenarios and report it in after-action reviews alongside standard network metrics.

Command Doctrine

Signal Officers advising commanders have a new planning requirement to introduce: Reaction Windows belong in the communications annex alongside frequency plans, call signs, and net assignments.

Defining which data types remain valid for how

Table 3

Scenario	Data Class / Window	PDR	TVDR (Class 3)	Current T&E Verdict
Low density (peacetime exercise)	Class 3 3–15 sec	93%	**~87%**	PASS
High density (wartime MUM-T)	Class 3 3–15 sec	82%	**0%**	PASS*
Any density	Class 0 (no expiry)	>95%	>95%	PASS

long is a command decision, and it needs to be made before the operation – not diagnosed after the network delivers information the fight has already moved past.

Conclusion

Military networks were designed to deliver information. They were never designed to enforce the time boundaries under which information is still valid for the current fight. The instinct is to prescribe faster networks. That misses the problem.

No amount of speed helps a network that cannot tell the difference between data still relevant to the current fight and data the fight has already moved past. Speed without that distinction just delivers the wrong picture more efficiently.

TGTA provides the missing mechanism. Class 0 data remains authorized indefinitely; Class 3 data loses its clearance in seconds. The system must know the difference; currently, it does not. Connectivity that arrives outside the authorization window – regardless of its technical quality – is not decision advantage. It is unauthorized input at machine speed.

Disclosure: *The author used Claude (Anthropic) artificial intelligence as a writing assistance tool for English expression, editing, and document formatting. Figure 1 was generated using Python/Matplotlib. All concepts, arguments, structural framework, simulation parameters, and source material originate exclusively from the author.*

References

Coram, R. (2002). Boyd: The fighter pilot who changed the art of war. Little, Brown.

Department of Defense. (2021a). MIL-STD-2045-47001E: Connectionless data transfer application layer standard. DoD.

Department of Defense. (2021b). MIL-STD-6017E: Variable Message Format (VMF). DoD.

Gady, F.-S., & Kofman, M. (2024). Making attrition work: A viable theory of victory for Ukraine. Survival, 66(1), 7–50.

Government Accountability Office. (2006). Military transformation: Army actions needed to better manage risks in developing capabilities for the Future Combat Systems (GAO-06-672). GAO.

Government Accountability Office. (2025). Defense command and control: Further progress hinges on establishing a clear JADC2 vision and requirements (GAO-25-106454). GAO.

NATO Command and Control Centre of Excellence. (2022). C2 agility in high-tempo scenarios: Lessons from BALTOPS. NATO C2COE.

Ricks, T. E. (2006). Fiasco: The American military adventure in Iraq. Penguin Press.

Shin, H. (2026). Structural time-admissibility as a safety interlock in networked systems. IEEE Access. https://doi.org/10.1109/ACCESS.2026.3679840

U.S. Army Training and Doctrine Command. (2024). Multi-domain operations lessons learned: Ukrai (TRADOC Pamphlet 525-92). TRADOC.

Author

Hyunkeun Shin is a principal researcher at the Korea Research Institute for Defense Technology Planning and Advancement (KRIT), Jinju, Republic of Korea, and retired lieutenant colonel, Republic of Korea Army Signal Corps, with 22 years of service in tactical C4I (Command, Control, Communications, Computers, and Intelligence) and data link systems. Shin is the author of a five-paper IEEE series on admissibility-governed networked and autonomous systems. He can be contacted at: honor58@naver.com

Restoring the Scholar-Warrior: A Shared Mandate for Students, Instructors, and the Signal School

Officers of Signal Basic Officer Leader Course, Class 003-26 approach the end of a 10-mile ruck ahead of a ceremonial regimental induction and pinning ceremony at Fort Gordon, Georgia, May 21, 2026. The ruck march is one of several milestones in the 16 weeks of intensive education and training encompassing the course.
(Photo by Laura Levering, U.S. Army Signal School)

Maj. Nicholas Christensen and Maj. William Sack
U.S. Army Signal School

Professional military education (PME) within the Signal Corps has become an easy target for criticism. Most signal officers, if honest, have likely said some version of the following during their company grade years and many continue to say it as field grade officers: "I did not learn anything at Signal Basic Officer Leaders Course," "Signal Captains Career Course was a waste of time," or perhaps the most common refrain, "It could have been done much better and focused on what actually mattered."

These comments are frequently voiced not only in private conversations among peers but openly in front of junior officers and senior leaders alike – and all were foolish to let them leave their lips before fully understanding the long-term impact. In retrospect, these statements reveal more about our misunderstanding of the purpose of institutional education than they do about the quality of the education itself. Perhaps "foolish" is a more academically appropriate term than "dumb," but the underlying point remains the same: such comments reflect a widespread misunderstanding of the role PME is intended to serve within the Army profession. PME was never designed to create fully trained experts for every future assignment; rather, it exists to develop adaptable officers capable of critical thinking, doctrinal understanding, and professional growth. While the former remains fully true, failing to acknowledge the shortcomings of the officers attending PME, the instructors tasked with teaching it, and the institution designed to create and manage it would be equally foolish. Expectations for officer PME should be high, and there are multiple places where change must occur quickly to meet the demands of a rapidly evolving landscape.

While this article focuses on signal captains PME, many of the recommendations are translated to other signal and non-signal officer courses. This

article argues that changes to all three are essential to creating a signal captain PME experience that produces officers ready to adapt to the demands of commanders tasked with executing in a modern warfare world and who are strategically minded, ethically grounded leaders capable of critical thinking and creative problem-solving (TRADOC, 2017, iii).

What Must Change for the Student

Before even arriving at Fort Gordon, Georgia, for the Signal Captains Career Course (SCCC), officers repeatedly hear the same advice: "This is your chance to take a break." In fairness, for many officers who attended during the mid-2010s, this mindset was shaped by nearly two decades of sustained conflict in Iraq and Afghanistan, combined with the operational and fiscal pressures imposed by the Budget Control Act of 2011, "Sequestration." By the time many officers arrived at SCCC, they genuinely needed a pause. The problem, however, is not the pause itself; it was its utilization. The intent of PME was never to provide an intellectual vacation characterized by passive learning and endless "doom scrolling," which often leaves individuals mentally exhausted rather than renewed. Instead, PME is intended as a focused professional pause: the opportunity to step away temporarily from the knife fight of day-to-day operations and re-engage intellectually at a level many officers have not experienced since their undergraduate education.

Unlike operational assignments, PME does not require continuous deployments, late nights in the office, or constant crisis management. It demands deliberate intellectual effort. This period provides officers with an opportunity to reconnect with Army doctrine, operational theory, and professional reflection before assuming the increased responsibilities associated with company command, battalion staff leadership, and future operational planning roles. Importantly, the institution recognizes its inability to fully prepare officers for every assignment they may encounter over the next six or seven years of company -grade service. Attempting to do so would require an impractical amount of time away from operational units, ultimately proving counterproductive. Instead, Army doctrine emphasizes self-development as a core component of leader growth.

Amy Regulation 350-1 identifies leader development as occurring across three domains: institutional, operational, and self-development (U.S. Department of the Army [DA], 2017). PME provides only one component of that framework. The individual officer bears responsibility for identifying personal weaknesses and deliberately pursuing growth through self-study, professional reading, certifications, mentorship, coaching, and technical education. Too often, officers approach PME seeking only the information necessary to pass exams, complete requirements, and move on. When officers reduce education to memorizing PowerPoint slides and utilizing CTRL-F to locate answers in regulations, the educational experience inevitably feels hollow. Under those conditions, it is unsurprising that officers later ask, "What was the point of that course?" Therefore, the paradigm must shift from the outset. Students should arrive at SCCC expecting academic rigor that challenges them to move beyond doctrinal familiarity to the ability to do genuine analysis, synthesis, and application.

PME must require officers to employ the critical thinking skills developed during undergraduate education and initial entry training, then refined through operational experience. Rather than merely identifying doctrinal answers, students must learn to apply doctrine within ambiguous operational environments and generate solutions to complex problems. Only then will the "focused professional pause" of PME achieve its intended purpose, better preparing officers for the unpredictable demands of future service.

What Must Change for the Institution

While individual officers bear substantial responsibility for their own professional development, the institution itself is not without fault. As centers of excellence standardize processes and U.S. Army Transformation and Training Command (T2COM) modernization efforts continue across the Army, the current environment presents a significant opportunity to reform how PME is designed and delivered. The Army must become more agile in developing curriculum, more selective in instructor assignments and preparation, and more willing to challenge officers intellectually beyond simple knowledge recall (U.S. Army Combined Arms Center [CAC], 2015).

Modernizing the POI Development Process

First and foremost, the program of instruction (POI) development process – specifically the ADDIE (Analyze, Design, Develop, Implement, and Evaluate) framework – requires modernization. The Army recognized this issue as early as 2015 when it established Army University, identifying a need to "revitalize the Army's professional military education system" (Command and General Staff College Foundation [CGSCF], 2015), yet in 2026 we still find articles calling for transforming Army education (Duckett, 2026).

While many strides have been made, the underlying curriculum development process remained largely unchanged. The ADDIE framework continued to operate on a deliberate multi-year cycle appropriate for an era of relatively stable technology and predictable modernization timelines. During much of the Global War on Terrorism (GWOT), this slower pace remained acceptable because technological change occurred incrementally and programs of record remained stable for extended periods. That environment no longer exists.

The pace of technological development, network modernization, and software integration now evolves

far faster than the institutional training pipeline is designed to accommodate.

The Army Operating Concept and Multi-Domain Operations framework both emphasize adaptability, rapid technological integration, and decentralized decision-making in contested environments while acknowledging the current gap in training (TRADOC, 2018, F-3). A five-year curriculum development cycle is no longer merely inefficient; it represents the operational risk of Signaleers unable to deliver critical data that enables a commander's ability to command and control the operation at the pace that the modern operational environment demands. As initiatives such as C2 Fix and C2 Now drive rapid capability changes across the Total Army, signal education must fundamentally shift from platform-specific instruction toward conceptual mastery.

Instruction can no longer center on specific systems such as the Command Post Node, Satellite Transportable Terminal, or legacy transport equipment. Instead, PME must focus on enduring concepts: networking, transport architecture, tactical communications integration, and systems interoperability. A signal officer does not necessarily need mastery of every individual system interface or modem configuration. Rather, officers must understand the principles underpinning communications architecture so they can rapidly adapt to whatever equipment set their unit possesses. The objective is not technical memorization, but operational adaptability.

Revitalizing the Instructor Corps

Second, the Army must restore prestige and rigor to instructor assignments within the Signal School: historically, instructor billets. Particularly, small group leader (SGL) positions were viewed as highly competitive and professionally rewarding assignments.

Instructors refined their doctrinal expertise while simultaneously gaining exposure to branch-wide modernization initiatives and institutional leadership at the enterprise level. At one time, prospective instructors interviewed directly with the Signal School commandant or the Signal Center of Excellence commanding general. This process reinforced the importance of the assignment and helped attract high-performing officers from diverse operational backgrounds, committed to contributing to the regiment. Likewise, programs such as Project Warrior created pathways for talented officers to influence the profession beyond their operational assignments. The ability to not only take their operational experience but also the collective knowledge gained from seeing multiple rotations of best practices and lessons learned is invaluable as an instructor. Together, these pathways – supported by an updated deliberate talent management process, with the assistance of branch career managers – must be a priority to properly develop future generations of Signaleers. During the GWOT era, however, operational experience became the dominant metric of professional value. Institutional assignments often became secondary considerations in officer career progression. As a result, the perception exists that the Army unintentionally devalued the very instructors responsible for educating the next generation of leaders. Reversing this trend is critical to producing officers able to meet the demands of future operational environments. Instructor preparation should include both advanced pedagogical training and technical expertise development.

While TRADOC Regulation 600-21 was updated in 2018 with the intent to formalize and improve instructor development, it is still a voluntary program and based upon observations that are still largely task-based training environments associated with Initial Entry Training rather than adult learning methodologies (TRADOC, 2018, 10-11). Yet, students in SCCC routinely receive graduate-level academic credit through civilian university partnerships. If the Army genuinely considers PME to be equivalent to graduate education, then instructor selection, preparation, and expectations must reflect that standard. Research on higher education consistently demonstrates that faculty quality is among the strongest predictors of educational effectiveness (Fink, 2008). Simply put PME's quality cannot exceed the quality of those entrusted to teach it.

Restoring Academic Rigor

Finally, the Army must address the issue of rigor within PME. A persistent culture exists in which PME is viewed as a period to "take a knee." Whether openly admitted or not, many officers have adopted this mindset because institutional expectations often reinforce it.

Too frequently, SCCC becomes an exercise in rememorizing the fundamentals and searching digital regulations rather than engaging in meaningful intellectual development. As technological complexity expands throughout the force, the requirement for officers to possess both tactical competence and technical understanding has never been greater. Future conflicts will demand leaders capable of integrating communications, cyber, data, and operational planning under contested conditions. Accordingly, signal PME must evolve in two significant ways.

First, academic standards must increase. Assessments must measure not only doctrinal familiarity but also analytical reasoning, operational application, and problem solving. Students will be challenged to think critically, conduct independent study, and engage deeply with course material beyond classroom hours. This necessarily requires moving away from simplistic open-note, multiple choice examinations toward assessments that demand synthesis of the information, written analysis, practical application, and the ability to evaluate outcomes.

Second, the institution needs to accept that not every student will succeed. For years, there existed an institutional reluctance to recycle or dismiss students from SCCC. While understandable from a personnel

management perspective, this approach undermines academic credibility and diminishes professional standards. PME cannot simultaneously claim graduate-level rigor while operating under an expectation of near-universal completion regardless of performance or effort. To achieve these objectives, a structural revision to PME would not only enhance academic rigor but also reduce permanent change of station (PCS) requirements, improve stability and predictability for officers and their families, and likely generate some long-term cost savings for the Army. A modernized adaptation of the former Advanced Course and Combined Arms and Services Staff School (CAS3) model could provide substantial benefits not only to the Signal Corps but across the broader Army profession.

By separating branch-specific technical instruction from a centralized common core curriculum, the Army could foster greater interdisciplinary collaboration and facilitate the exchange of lessons learned across warfighting functions. This type of approach would further strengthen branch technical education by ensuring it is grounded in a foundational understanding of FM 3-0 and the principles of multi-domain operations. Officers would then arrive at their branch-specific courses with a shared operational framework, enabling instruction to focus less on doctrinal familiarization and more on analysis, integration, and application within complex operational environments.

Conclusion

The Army currently operates in a strategic environment that is both familiar and unprecedented. While the profession continues to face timeless leadership challenges, modern warfare increasingly demands new intellectual approaches capable of addressing rapidly evolving technological and operational realities.

Gen. John Murray warned, "We do not want to get to 2035 to find we have fallen behind. We want to aim ahead of the competition and not behind it" (Murray, 2021). If this warning is interpreted solely through the lens of technology acquisition, then the Army misunderstands the deeper issue entirely.

Technological superiority alone does not guarantee military advantage. The Army's decisive advantage has always been its people. If Soldiers truly remain the Army's greatest asset, then the Army must critically reassess how it educates its officers. Officers entering PME must arrive prepared to engage intellectually, challenge themselves academically, and deliberately build the professional toolkit required for future leadership. Simultaneously, the institution must evolve to support that expectation through increased rigor, better instructors, more adaptable curriculum development, and a renewed emphasis on critical thinking.

Ultimately, PME exists not simply to transmit information, but to cultivate adaptable leaders capable of thinking under conditions of uncertainty.

William Butler perhaps captured this relationship best when he warned: "The society that separates its scholars from its warriors will have its thinking done by cowards and its fighting done by fools."

References

Butler, W. F. (1889). *Charles George Gordon* (p. 85).

Command and General Staff College Foundation. (2015, July 8). *The Army establishes The Army University*.

Duckett, D. (2026, March 27). *Transforming Army education: The leadership laboratory*. Small Wars Journal.

Fink, O. J., Jr. (2008). *Professional faculty development in the military education system* (Art of War Studies Military Issues Paper). U.S. Marine Corps Command and Staff College.

Murray, J. M. (2021, March 17). *Keynote address* [Speech]. AUSA Global Force Next Virtual Symposium.

U.S. Army Training and Doctrine Command. (2017). TRADOC Pamphlet 525-8-2: *The U.S. Army Learning Concept for Training and Education*. Headquarters, Department of the Army

U.S. Army Training and Doctrine Command. (2018). TRADOC Pamphlet 525-3-1: *The U.S. Army in Multi-Domain Operations 2028.* Headquarters, Department of the Army.

U.S. Army Training and Doctrine Command. (2019). TR 600-21 *The Army School System (TASS).* Headquarters Department of the Army.

U.S. Department of the Army. (2017, December 10). *Army training and leader development* (Army Regulation 35 0-1).

Maj. Nicholas Christensen serves as the executive officer for the U.S Army Signal School Commandant and Chief of Signal. Prior to his current assignment, he was the deputy commander for the 22nd Corps Signal Brigade. Christensen has held diverse command and staff positions across both Army and joint units, supported by multiple deployments to the Middle East.

Maj. William Sack serves as branch chief for the Signal Captains Career branch of the U.S. Army Signal School. Prior to his current assignment, Sack was executive officer for 114th Signal Battalion. He has held diverse positions across the Army, supported by varied operational leadership roles.

Photos that did not make the cover but we believe are cover-worthy!

Spc. *Isaiah Hopson (left) and Cpl. Rahzell Wilson, 1st Mobile Brigade Combat Team, 101st Airborne Division (Air Assault), configure an on-the-move network node during Signal Mobile Advanced Readiness Training at Fort Campbell, Kentucky, on May 20, 2026. (Photo by Chief Warrant Officer 5 Paul Sankey, U.S. Army Signal School)*

Have what it takes to make the cover?

Photos must be ***a minimum*** 1MB resolution (higher is better) and feature at least one Soldier. Include Soldier's **rank, full name**, and **unit** along with brief **description** of photo. Due to the publication's format, vertical shots (versus horizontal) have a greater chance of being considered for the cover. Got questions? Ask! → Laura.M.Levering.civ@army.mil

Pfc. Crystal Sialoi, 57th Expeditionary Signal Battalion-Enhanced, 11th Corps Signal Brigade, undergoes Signal Gunnery certification for deployment to Poland. (Photo by Spc. Jovanni, Headquarters and Headquarters Company, 11th CSB)

Submission guidelines *at a glance*:

- Word document, between 500 and about 2,000 words.
- Use **APA** format when citing sources.
- Photos/graphics must be **separate attachments** (not embedded in Word)**.** Each needs a **brief description** along with the **rank, full name**, and **unit** of person who took photo (created graphic).
  - Acceptable formats: **.jpg** or .**png**
- **Spell out acronyms** on **first** reference followed by acronym in parenthesis; use acronym on subsequent reference.
- Include **short bio** and **photo** if possible (see other published articles for example).
- ***Questions***? Reach out: laura.m.levering.civ@army.mil

LINE OF DEPARTURE
CONNECTING U.S. ARMY PROFESSIONALS TO THE BEST PROFESSIONAL WRITING

⇒ **Centralized hub for Army branch journals**

⇒ Web-first, mobile-optimized HTML

⇒ All articles available in audio format

⇒ Site is optimized with SEO metadata