ARMY COMMUNICATOR

THE PROFESSIONAL BULLETIN OF THE U.S. ARMY SIGNAL REGIMENT | FALL 2026

Connecting Our Past • Powering Our Present • Securing Our Future



Approved for public release; distribution is unlimited. | Headquarters, Department of the Army | PB 11-26-4



Table of Contents

3 | Leadership Makes the Difference
Col. Bernard Brogan

5 | Shared Development
Institutional and Operational Responsibilities
Command Sgt. Maj. Lisa M. Gandy

6 | Beyond Buttonology
Building Communicators Who Understand the Network
Chief Warrant Officer 5 Willie L. Newkirk

9 | Editor's Note
Laura Levering

10 | Trust As the Bedrock of the Signal Corps
Chaplain (Maj.) Glen Thompson

12 | The Network Is In The Fight
Shifting the Signal Officer's Role
Capt. Augustine Tengey

15 | Burden of Leadership
What the Profession of Arms Requires of Leaders
Lt. Col. Terrance "TP" Pitts

17 | DISA as a Service Member
The Backbone of Modern Battlespace
Sgt. 1st Class Preston W. LaRue

19 | Breaking the Box
Self-Modernizing WIN-T Stacks to Fight Tomorrow's Wars
Col. Kurt W. Page and Capt. Noah R. Ogrydziak

24 | Rebuilding S6 for Decision Dominance
Maj. Aaron S. Fernandez

28 | Modernizing the CGSC's Wireless Network
A Blueprint for Data-Centric Curriculum
Maj. James Jagozinski and Peter Cerny

30 | Standardizing Military Installation Resilience
From the Foundation to the Firewall
Larry Poole

33 | 'From the Edge to the Enterprise'
Signal Corps welcomes 44th Chief of Signal
Laura Levering

U.S. Army Signal Corp Leadership:
Col. Bernard Brogan
44th Chief of Signal and U.S. Army Signal School Commandant

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

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

Army Communicator:
Laura Levering
Editor-in-Chief / Harding Fellow
Send articles, photos, graphics, and story ideas for the Army Communicator to the editor-in-chief at laura.m.levering.civ@army.mil.

Layout and design support provided by Army University Press.

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.

Cover photo: *Soldiers assigned to the 304th Expeditionary Signal Battalion-Enhanced install and inspect communications equipment in support of Ulchi Freedom Shield at CP Tango, Aug. 11, 2026. These complex, all-domain exercises build credible deterrence by ensuring our combined forces are ready to communicate, coordinate and respond decisively to any threat.* ***(U.S. Army photo by Cpl. Shin Haegyeom, 1st Signal Brigade)***



Leadership Makes the Difference

On July 31, 2026, I assumed responsibility as the 44th Chief of Signal and Commandant of the United States Army Signal School. In the months since taking the colors, my visits across tactical formations, classrooms, and development centers have reinforced one consistent truth: The dedication and talent of our Soldiers, noncommissioned officers, commissioned officers, warrant officers, and Department of the Army civilians remain our greatest strategic advantage. Yet as the operational environment grows increasingly complex, our institutional approach must adapt to meet the speed and demands of the future fight.

From day one, my guidance to the Signal Regiment has centered on a single, non-negotiable imperative: **To meet the demands of today's contested battlefields, we must expand upon our proud Signal heritage as warfighting Communicators who deliver decisive command and control across the joint battlespace.**

The Army cannot rely on technicians who only manage hardware or monitor circuits in isolation. Large-scale combat operations against peer adversaries demand leaders who master the operational environment, exercise sound operational judgment, and bring together data, transport, and spectrum at the critical time and place. The unified network is not a passive support mechanism; it is a decisive combat capability and an essential warfighting platform. Our operational culture must embody that reality across every echelon.

Across Fort Gordon, our training developers and cadre are already executing this mandate. They are comprehensively updating legacy programs of instruction, integrating hands-on operational scenarios, and ensuring our curriculum reflects the realities of multi-domain operations. The drive, candor, and technical agility demonstrated by our students are already reshaping our classrooms.

As we enter fiscal year 2027, our modernization efforts will focus along four primary lines of effort:

Priority 1: Modernize Institutional Instruction Across All Cohorts

Modernization is meaningless if it fails to reach the classroom floor. We are actively synchronizing courseware with fielded programs of record, integrating cutting-edge software suites, and ensuring instructors possess the advanced technical credentials required for modern warfare. Our Soldiers deserve training that reflects operational conditions rather than legacy paradigms.

Priority 2: Instill and Enforce the Culture of the Communicator

Culture is anchored in disciplined leadership and reinforced through mentorship. Professional military education must produce leaders who understand the direct tactical effects of communication on combined arms maneuver. We must move beyond segmented technical tasks and teach the interconnected battlefield reality of data distribution, resilient transport, electromagnetic spectrum operations, defensive cyberspace operations, and tactical survivability.

Priority 3: Deepen Strategic and Operational Integration

The institutional schoolhouse cannot operate in a vacuum. We are broadening closer collaboration across operational formations, commercial industry leaders, academia, and Army modernization cross-functional teams. Signal School graduates must arrive at their units ready to immediately employ emerging architectures, adapt to contested electronic environments, and accelerate tactical readiness without requiring remedial field training.

Priority 4: Improve Systems to Support Decisive Action

The speed and precision our missions require are often slowed by outdated processes and unnecessary administrative layers. To strengthen readiness and keep pace with the Army's demands, we will take a thoughtful look at the policies and systems that hold us back.

Throughout FY27, we will focus on reducing friction, simplifying procedures, and giving leaders the clarity and freedom they need to execute with confidence. By refining how we operate at both enterprise and tactical levels, we'll enhance agility, reinforce mission command, and better position the Regiment to deliver at the speed the fight requires.

Fiscal year 2027 marks a defining chapter for the Signal Regiment. By discarding outdated paradigms and aggressively modernizing our people, processes, and doctrine, we ensure the United States Army maintains an unassailable decision advantage. Our focus is simple: Build communicators who understand the fight, enable commanders, and deliver the network when and where it's needed. Together, we will build, train, and field the decisive Communicators our Army requires to fight and win.

Col. Bernard Brogan,
44th Chief of Signal and U.S. Army Signal School Commandant



Shared Development

Institutional and Operational Responsibilities

Moving beyond buttonology cannot occur solely within the walls of the Signal Schoolhouse. Institutional training provides the foundation; however, operational formations must develop, reinforce, and sustain that baseline to achieve true mastery.

Strategic readiness demands that leaders prioritize mission-essential training. We achieve organizational excellence by combining continuous professional development with hands-on experience, honest reflection, and clear accountability. For the Signal Regiment, this means technical development cannot end at graduation. Commanders, command sergeants major, signal leaders, warrant officers, noncommissioned officers (NCOs), and technical experts must actively collaborate to create environments where Signaleers continuously develop their craft. This requires designing and executing meaningful technical training that includes:

- Rigorous troubleshooting repetitions under time pressure
- Detailed technical network rehearsals prior to field operations
- Simulating degraded, intermittent, and denied communications
- Operating under contested electromagnetic spectrum conditions
- Injecting realistic, simulated cyberspace threats into training scenarios
- Enforcing periods of reduced reach-back and simulated outages
- Implementing a structured reduction of external technical support to build self-reliance and confidence in skills

Most importantly, leaders must require technicians to explain *why* a technical solution works, rather than simply demonstrating *that* it works.

As our technical leaders and trusted advisors, warrant officers play a critical role in the development of our Signaleers across the Regiment. The value of a warrant officer cannot be measured solely by their individual ability to personally solve the hardest technical problem in the formation. If every difficult network issue is immediately handed off to the warrant officer, the network may be restored, but a vital developmental opportunity has been missed. Rather, our warrant officers must focus on developing the technical capacity of the Soldiers and NCOs around them.

Instead of taking over the keyboard, technical leaders should ask these questions to develop the technical expertise of their Signal Soldiers and NCOs:

- What symptoms are they currently seeing on the network?
- What should be happening, according to the network design?
- Where is the physical or logical failure most likely to exist?
- What diagnostic evidence supports their technical assessment?
- What specific test would they execute next and why?
- What is the immediate operational impact?

By guiding the Soldier toward the solution rather than automatically becoming the solution, technical leaders ensure that their individual expertise creates more technical expertise across the entire formation.

Ultimately, today's fight requires a fundamental cultural shift from passive troubleshooting to active, cognitive engineering. True readiness is not manufactured in the classroom alone; it is forged daily in the operational dirt through shared institutional foundations and rigorous, realistic unit training. When we invest in developing the technical depth of our junior Soldiers and NCOs, we do not just fix the network – we build the agile, confident, and resilient technical warfighters required to dominate the modern battlefield.

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

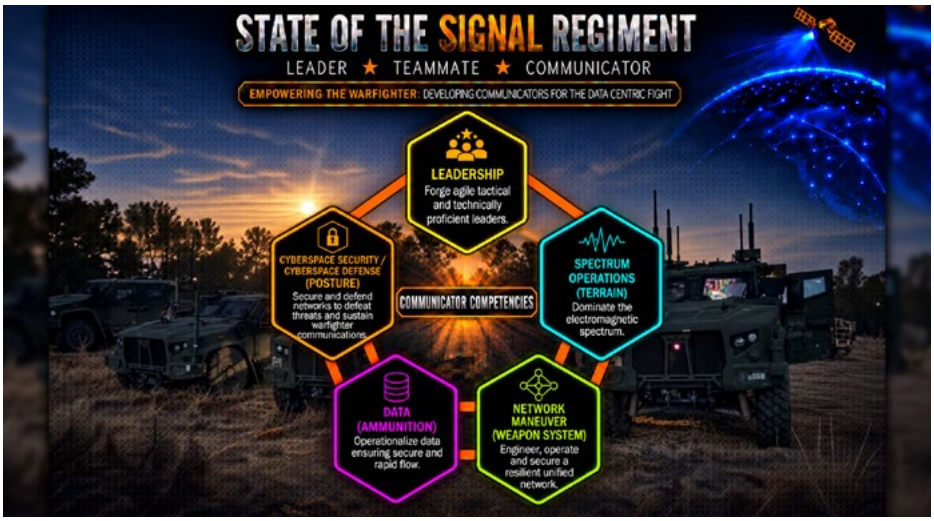


Beyond Buttonology

Building Communicators Who Understand the Network

Technology will continue to change, but the fundamentals cannot. Tactical forces are preparing for an operational environment shaped by large-scale combat operations (LSCO), contested communications, and the integration of space, cyberspace, electronic warfare, data, and artificial intelligence (AI) into command and control (C2). For the Signal Regiment, the network must be understood and employed as a weapon system. It delivers the data that powers C2 and enables commanders to see, understand, decide, direct, and assess. Without resilient C2, individual weapon systems become isolated, and the joint force loses its ability to synchronize operations across domains. The network delivers data, data enables decisions, and decisions win battles.

This mission requires more than Communicators who can turn on a system, follow a checklist, establish connectivity, and verify communications. Today's Communicators must understand what happens after they push the button. They must know how data moves, why routes converge or fail, how transport capabilities interact, how systems authenticate and exchange information securely, and how networks are engineered, operated, secured, and sustained. Cyberspace defense professionals must also understand how to identify and respond to adversary activities. This technical mastery directly strengthens the Regiment's ability to deliver resilient C2 and reliable support to the warfighter when the expected answer is absent from a manual, checklist, or AI-generated response.



Infographic prepared by Chief Warrant Officer 5 Willie Newkirk and Lt. Col. Nancy Tucker, U.S. Army Signal School, with assistance from ChatGPT (OpenAI).

The Next War Will Not Give Us the Answer Key

Future conflicts will not mirror the recent past. In LSCO, formations should expect degraded, intermittent, and limited communications; a contested electromagnetic spectrum; persistent cyberspace threats; disrupted physical and logical transport; frequent displacement; reduced reach-back; and adversaries seeking to disrupt, exploit, degrade, or deny C2. Because the Army never fights alone, these challenges will affect joint, interagency, coalition, and industry partners operating across a shared mission environment.

Failures in this environment may not present familiar error codes, and contractors or field service representatives may not be available. Manuals may not address the ad hoc mix of military, joint, coalition, and commercial technologies; cloud services; satellite and terrestrial transport; wireless capabilities; and software-defined architectures employed in the field. Because the enemy gets a vote, Communicators must understand engineering and architecture well enough to diagnose unexpected problems, reconfigure networks, secure vulnerable systems, restore services, and sustain the commander's ability to command and control. Cyberspace defense professionals require additional expertise to recognize malicious activity, assess mission impact, respond to incidents, and mitigate adversary actions.

Fundamentals Create Adaptability

Technical fundamentals are not merely basic skills. They are enduring principles upon which advanced capabilities depend. Required depth varies by military occupational specialty, grade, and billet, but all Communicators need a foundation in:

- Internet Protocol networking, addressing, subnetting, routing, switching, and transport;
- Data flows, systems administration, identity and access management, and network management;
- Cyberspace security and systematic troubleshooting;
- Electromagnetic spectrum operations, virtualization, cloud computing, and the relationships among applications, services, infrastructure, transport, and data.

These foundations allow Communicators to adapt across platforms without treating each technology as an entirely new profession. A Communicator who understands routing can learn a new manufacturer's device. One who understands networks and data flows can adapt to software-defined and cloud architecture. Security fundamentals help personnel secure unfamiliar technologies, while knowledge of architecture, defensive methods, and threat behavior prepares cyberspace defense professionals to recognize and respond to adversary activity.

Data literacy is equally important because data creates decision advantage only when commanders can access and trust it. Secure, governed data environments must preserve data quality, source, availability, and appropriate access so leaders can make faster, better-informed decisions at every echelon. Trusted data enables trusted decisions. The platform and threat will change. The fundamentals endure.

Distinguishing Cyberspace Security (Cybersecurity) from Cyberspace Defense

Cyberspace security and cyberspace defense are complementary, but they are not synonymous. Cyberspace security consists of the proactive measures used to securely configure, operate, manage, and protect systems and networks. It includes access controls, configuration and vulnerability management, governance, compliance, auditing, and maintaining the confidentiality, integrity, and availability of systems and data. Every Communicator must apply the security requirements associated with their duties. Cyberspace security is not merely an administrative function. It is a condition of combat readiness that preserves the network, protects trusted data, and sustains the combat power C2 enables.

Cyberspace defense is threat-focused and requires specialized personnel, training, capabilities, and authorities to identify malicious activity, analyze threats, respond to active intrusions, and mitigate adversary actions against the network and the mission it enables. Recognizing where administrative security ends and active defense begins helps units escalate incidents appropriately and preserve operational integrity. Cybersecurity reduces exposure and strengthens the environment; cyberspace defense counters active threats. Together, they preserve combat power by keeping commanders connected and by protecting the data and services required to fight.

Troubleshoot the Network, Not the Checklist

Troubleshooting is one of the clearest demonstrations of technical understanding. Rather than repeat procedures when prescribed actions fail, a Communicator grounded in fundamentals asks diagnostic questions:

- Where does the data originate, where should it go, and what path should it take?
- Which transport, infrastructure services, authentication points, and network segments are functioning?
- What configuration or environmental conditions changed?
- Is the failure related to routing, transport, spectrum, hardware, software, identity, security, or a service?
- Could the behavior indicate malicious activity requiring escalation to cyberspace defense personnel?
- What is the immediate effect on the commander's mission?

These questions turn troubleshooting into disciplined reasoning. They develop Communicators who can isolate failures, select the next meaningful test, and restore capability under pressure.

Interoperability by Design

Interoperability wins wars because the Army never fights alone. The network must enable seamless operations with joint, interagency, coalition, and industry partners from the first day

of a crisis or conflict. That capability depends on compatible architecture, data standards, identity and access controls, transport pathways, mission-partner environments, and rehearsed procedures. Interoperability must be designed, engineered, secured, and tested from the beginning. It cannot be added after systems are fielded or after operations begin. Communicators who understand the network can identify integration risks early, translate requirements across organizations, and ensure data reaches the right decision maker at the required speed and classification.

AI Must Amplify Expertise

AI can assist with network monitoring, anomaly identification, configuration analysis, predictive maintenance, knowledge management, troubleshooting, cyberspace security, cyberspace defense, and threat analysis. Communicators should learn to use these capabilities effectively and responsibly, but AI must not become a high-tech form of buttonology. Blindly implementing a machine-generated recommendation merely replaces a paper checklist with a digital one.

Technical professionals must determine whether a recommendation makes sense in engineering, fits the tactical architecture, introduces operational or security risk, relies on faulty assumptions, or requires escalation to another specialty. They must also retain a contingency plan if the recommendation fails. As automation grows, so does the need for professionals who understand what technology is doing. AI should amplify human expertise and judgment, not replace them.

Building Communicators Ready to Fight and Win

Platform-specific training remains necessary, but it must be paired with the science beneath the equipment, the logic behind configurations, the movement and governance of data, interoperability requirements, and deliberate opportunities to apply knowledge under pressure. Communicators must learn to operate and secure the systems for which they are responsible. Cyberspace defense professionals must develop the specialized ability to recognize malicious activity, assess mission impact, respond within their authorities, and take appropriate defensive action. Training should purposefully break networks, degrade data availability, challenge mission-partner connections, and introduce unfamiliar technologies so personnel must reason, adapt, integrate, and recover.

Readiness is measured by whether formations possess the collective expertise to engineer, operate, secure, defend, troubleshoot, integrate, adapt, and sustain networks in contested conditions while continuously supporting the warfighter. A resilient network connects formations and weapon systems, delivers trusted data, enables decision advantage, and allows the joint force to synchronize operations. Every secured and defended network preserves combat power. The Signal Regiment has always adapted alongside technology – from flags and telegraph wire to radio, satellites, data networks, cloud computing, and AI. Its enduring responsibility remains enabling commanders to command and control their formations.

Equipment and threats will continue to evolve. Our Communicators must evolve faster than both. Teach them which button to push, but also teach why the network works, how data powers decisions, how partners connect, how to determine why the network does not work, and how to fight through the problem when technology, the environment, or the enemy changes. That is how we move beyond buttonology, preserve combat power, and remain ready to support the warfighter.

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



The deadline to submit articles for the Winter 2026 Army Communicator is Dec. 11*. However, you are encouraged to submit early. The sooner your article is received, the more likely it is to be published.*

Contact Laura Levering directly via Microsoft Teams or email with questions or concerns.

Quick Links:

1. Line Of Departure
2. How To Get Published
3. Army Communicator Submission Guidelines

Editor's Note

In the Summer 2026 Army Communicator, I noted that future editions would feature changes. Some of those changes begin with this issue, including a new layout and fewer articles. The reasons for these changes extend beyond what is visible in this issue.

As the professional bulletin of the U.S. Army Signal Regiment and U.S. Army Signal School, we must continue to evolve with the Army. One thing that will not change is my commitment to helping "get the message through." Publishing fewer articles each quarter does not mean less work; in some cases, it means more. It means I will be more intentional in my copyediting and providing feedback. It means working with authors to publish articles (and accompanying photos/graphics) that reach readers, rather than publishing simply for the sake of publication.

Everything we do is to help encourage professional military discourse – the core purpose of the Harding Project and reason behind this effort to revitalize professional journals. I'll admit I was skeptical when the initiative was first introduced. Nearly three years later, I am beginning to see a return on investment and am reminded that change (typically) does not happen overnight. We have evolved from a publication largely filled with news articles and white papers to one featuring thoughtful pieces that challenge readers to think about issues, and in some cases, respond with an article proposing solutions.

During an annual Harding Project workshop in September, Sgt. Maj. of the Army Michael R. Weimer shared several points that resonated with me and other branch journal staff. An advocate for professional discourse, the senior enlisted leader acknowledged that writing does not always come easily for Soldiers – himself included. Effective writing requires critical thinking, which sometimes involves taking risks. However, it is a risk worth taking when the topic has the potential to benefit the Army. "We are encouraging people to write more in the way we communicate," Weimer said. "There is a way to write that is both provocative but not offensive." Rest assured, we will not publish content that could place a Soldier-author in jeopardy. At minimum, three people (your supervisor, me, my chain of command) should review and potentially revise your work before it is published.

Now that we have moved away from quarterly themes, what topics should authors consider that encourage professional discourse? I believe Weimer said it best during the conference. His advice: Focus on the things that you are passionate about. Leader development, physical training, your specific military occupational specialty/branch, taking care of Soldiers, training, health and wellness, emerging technology, lessons learned … there is no shortage of things in this profession that people are passionate about. Grab a hold of that "thing," and type your thoughts. Sometimes discussing the topic with someone first helps. Create an outline of what you want to share, then begin writing. If the words are not flowing, set what you have aside and return to it later; don't wait too long though. See it through, and before submitting a draft, have someone else read it first.

Visit Line of Departure regularly to read how other Soldiers are contributing to their professional publications. Download the Line of Departure app! You will have access to all U.S. Army journals, featured articles (including Recommended Articles of the Month), writing tips, videos and more – all from the palm of your hand.

Laura Levering
U.S. Army Signal School



Trust As the Bedrock of the Signal Corps

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

Army Doctrine Publication (ADP) 6-22, Army Leadership and the Profession, establishes trust as the bedrock of our profession. For Army Signaleers, this principle takes on a critical dual significance. Trust is the interpersonal glue that builds cohesive units. It is also the fundamental assurance that commanders will maintain the command and control required to fight and win.

Mutual Trust at the Tactical Edge

ADP 6-22 defines mutual trust as shared confidence between commanders, subordinates, and partners. In the Signal Corps, this shared confidence is tested daily at the very edge of the battlefield. Signaleers frequently operate in decentralized, small-team elements – such as a retransmission team isolated on a high-elevation point or a small network operations cell supporting a tactical command post. In these austere environments, leaders must place immense trust in junior Soldiers to configure, maintain, and troubleshoot highly complex systems without direct, constant supervision. This trust is not given blindly; it is earned through rigorous training and a demonstrated ability to execute the mission under pressure. When a leader trusts a subordinate to manage the network, they empower that Soldier to act decisively in the absence of orders.

Competence and Commander's Confidence

Trust in the Signal Corps extends outward to the supported maneuver commander. A commander's trust in their Signaleers is intrinsically linked to the

Army Doctrine Publication 6-22 (Army Leadership and the Profession) establishes core principles, attributes, and competencies for Soldiers and Army civilians. View and download ADP 6-22, along with other ADPs, here: https://armypubs.army.mil/productmaps/pubform/adp.aspx

concept of competence, which ADP 6-22 identifies as a core component of building trust. A Signaleer must be a master of their craft – understanding not just the physical hardware, but the data flow, cyber threats, and operational picture. When the network is resilient and reliable, the commander trusts in their situational awareness and can make rapid, lethal decisions. If that technical competence wavers, the commander's trust erodes, directly compromising the combat effectiveness of the entire formation.

Character and Commitment

Alongside competence, ADP 6-22 highlights character and commitment as essential pillars of trust. For Signaleers, character is demonstrated through uncompromising integrity: handling sensitive information properly, strictly adhering to communications security protocols, and reporting network vulnerabilities honestly, even when it is inconvenient. Doing the right thing when no one is watching is the hallmark of a trusted network defender.

Commitment is equally vital. It is a dedication to battle fatigue, stay awake through the night, and endure harsh elements to restore a critical data link. Commitment drives Signaleers to tirelessly purse keeping the network operational because they know that somewhere, a Soldier's life depends on that transmission getting through.

Key Takeaway

Trust is the unseen frequency upon which the entire Signal Corps operates. As outlined in ADP 6-22, it requires a continuous, deliberate effort to cultivate through character, competence, and commitment. For Army Signaleers, building mutual trust within their teams and maintaining the trust of their commanders is as critical as any piece of hardware. The Signaleer who embodies this trust ensures that the Army remains connected, lethal, and ready for any mission.

About the Author



Chaplain (Maj.) Glen W. Thomspon is the ethics and regimental chaplain for the U.S. Army Signal School at Fort Gordon, Georgia, where he advises leadership on morals and leads ethical instruction for the Signal Regiment. A native of Staten Island, New York, who grew up in Blackwood, New Jersey, Thompson's key previous assignments include serving as the brigade chaplain for the 25th Infantry Division Artillery (DIVARTY) at Schofield Barracks, Hawaii, and as the battalion chaplain for both the 56th Signal Battalion and the 5-20th Infantry Regiment at Joint Base Lewis-McChord, Washington. His operational experience includes combat deployments to Afghanistan in 2012, and Iraq in 2015. Outside of his military ministry, Thompson enjoys traveling and participating in outdoor sports with his wife and their four children.



The Network Is in the Fight

Shifting the Signal Officer's Role

Capt. Augustine Tengey
41st Field Artillery Brigade

Disclosure: The author used Claude (Anthropic) as an editorial aid to format citations.

A communications system can be fully operational, and a unit can still be unprepared to fight without it. That distinction matters as the Army prepares for large-scale combat operations (LSCO) against adversaries that can disrupt networks, locate electromagnetic signatures, and attack command posts (CPs).

Modern formations depend on radios, tactical networks, satellite communications, and digital command and control (C2) tools to move information and coordinate operations. Those systems give commanders speed and visibility, but they also create dependencies.[1] Therefore, the Signal Corps should measure success by more than network availability. The more useful question is whether a formation can continue C2 when the preferred network is degraded, denied, or destroyed. That is a command problem, not simply a signal problem.

Communications: A Part of C2

Army doctrine describes C2 as the means by which commanders understand situations, make decisions, direct actions, and lead forces. Communications provides pathways that connect those activities across a formation.[2] When those pathways fail, the effect is not limited to the S-6 or signal section. Delays appear in reporting, orders, fires, intelligence, sustainment, and coordination with higher and subordinate headquarters. This is especially important for field artillery. A firing unit

The Joint Network Node team from 41st Field Artillery Brigade works to establish network connectivity for the tactical operating center. ***(Photo by Capt. Augustine Tengey, 41st Field Artillery Brigade)***

depends on timely information to receive targets, process missions, coordinate with supported formations, execute fires, and assess effects. Current field artillery doctrine emphasizes the rapid, continuous integration and synchronization of fire support capabilities.[3]

If information cannot move at the required speed, the formation may possess capable weapons but lose the ability to employ them at the right time. That is why commanders should treat communications as part of their C2 architecture from the beginning of planning. The communications plan should answer an operational question: What must the unit still be able to do when the primary network is unavailable?

Survivability Starts Before the Network Fails

The Army's network modernization effort has expanded the number and type of communications pathways available to tactical formations. The Integrated Tactical Network, for example, is intended to provide a more flexible tactical network by integrating multiple transport and communications capabilities.[4] More options can improve resilience, but additional systems also require power, trained personnel, configuration, maintenance, and disciplined employment.

The problem becomes sharper at the CP. Recent Army professional writing has described CPs as increasingly vulnerable because their physical and electromagnetic signatures can reveal their location to an enemy. Communications is part of that signature.[5]

A headquarters that concentrates personnel, antennas, generators, vehicles, and digital infrastructure in one location may gain efficiency while increasing its risk of detection and attack. Commanders do not need to become network engineers to manage this risk. They do need to know which communications capabilities are essential, what alternatives exist, how long the staff can function with degraded services, and which C2 functions have priority. A PACE plan (primary, alternate, contingency, emergency) is only useful when the commander understands what each option can support.[6]

Training for Degraded Communications

A unit should not discover its communications weaknesses during combat. Degraded communications should be deliberately built into collective training.

During a CP exercise, leaders can remove a primary service and require the staff to continue the battle rhythm. During a field exercise, a unit can limit bandwidth or take a network node out of service. During a rehearsal, subordinate units can practice receiving essential orders through alternate methods. During an after-action review, leaders can ask a question that goes beyond equipment status: Did the formation maintain C2?

This approach changes the purpose of communications training. Instead of measuring whether a radio can transmit or a network can pass traffic, the unit measures whether commanders and staff can continue the mission when the preferred system is gone. Army experience with CP survivability reinforces the need for this type of training. The vulnerability of large, detectable CPs has been identified as a major challenge in LSCO, and Army authors have argued that future CPs must become more agile, resilient, and adaptable without sacrificing the ability to support the commander.[7] Communications must be included in that discussion because a highly mobile CP that cannot maintain essential information flow is not necessarily more survivable; it may simply be less capable.

S-6 as an Operational Advisor

This environment also changes what commanders should expect from their signal officers. The S-6 should not be limited to reporting that a system is "green" or "red." The more valuable report explains the operational consequence.

If a satellite link is degraded, what functions are affected? Which subordinate units can still be reached? What information can move? What cannot? How long can the formation operate under the degraded condition? What decision or mission is at risk?

Those questions require the signal officer to understand the commander's priorities, the staff's battle rhythm, and the formation's mission-essential tasks. Field Manual 6-02 places signal support within the broader operational environment and emphasizes the need for communications capabilities that support Army operations under changing conditions.[8] The S-6 should therefore participate in mission analysis, rehearsals, CP exercises, and risk discussions – not because the S-6 replaces the operations staff, but because communications conditions can directly change what the formation can accomplish.

Practical Standard for Commanders

Commanders can make this shift without adding another complicated assessment program. Four questions are enough to start.

What communications capabilities are essential to the mission?

What happens if each one is lost?

What is the unit's best alternative, and has it been rehearsed?

Can the formation continue to make decisions, issue orders, coordinate fires, and receive critical reports while degraded?

These questions move communications out of the technical annex and into the commander's decision space. They also establish a clearer purpose for the signal officer: helping formations preserve C2 when those connections are contested, rather than merely keeping systems connected.

Conclusion

The Army's communications challenge is no longer simply connecting more users to better networks. It is learning how to fight when those networks are under pressure.

A reliable network gives commanders an advantage. A resilient communications architecture gives commanders options when the network is disrupted. Rehearsing those options through training converts them into capability.

For the Signal Corps, the implication is straightforward: Communications should be treated as a combat function that contributes directly to survivability, decision-making, and operational tempo. For commanders, the standard should be equally straightforward: Do not ask only whether the network works. Ask whether the formation can still fight when it does not.

About the Author

Capt. Augustine Tengey is an Army signal officer currently serving as the battalion communications staff officer for 1st Battalion, 77th Field Artillery Regiment, 41st Field Artillery Brigade, in Germany. He holds degrees from the University of Eastern Finland and Western Governors University. His professional experience includes strategic and tactical communications, mission command systems, and communications support for sustainment and field artillery operations.

References

1. Department of the Army. (2019). *Field Manual 6-02: Signal support to operations*. Headquarters, Department of the Army; Department of the Army. (2019). *Army Doctrine Publication 6-0: Mission command: Command and control of Army forces*. Headquarters, Department of the Army.
2. Department of the Army. (2024). *Field Manual 3-09: Fire support and field artillery operations*. Headquarters, Department of the Army.
3. Blumberg, M. S. (2020). The Integrated Tactical Network: Pivoting back to communications superiority. *Military Review, 100*(3), 104–110.
4. Beagle, M. H., Slider, J. C., & Arrol, M. R. (2023). The graveyard of command posts: What Chornobaivka should teach us about command and control in large-scale combat operations. *Military Review, 103*(3), 10–21. https://www.armyupress.army.mil/journals/military-review/english-edition-archives/may-june-2023/graveyard-of-command-posts/
5. Broyles, C. A., & Richter, C. H. (2023). Concrete command: Why combat training centers should prioritize training on urban command posts. *Military Review, 103*(4), 12–20. https://www.armyupress.army.mil/journals/military-review/english-edition-archives/july-august-2023/concrete-command/
6. Department of the Army. (2019). *Field Manual 6-02: Signal support to operations.* Headquarters, Department of the Army.
7. Beagle, M. H., Slider, J. C., & Arrol, M. R. (2023). The graveyard of command posts: What Chornobaivka should teach us about command and control in large-scale combat operations. *Military Review, 103*(3), 10–21. https://www.armyupress.army.mil/journals/military-review/english-edition-archives/may-june-2023/graveyard-of-command-posts/
8. Department of the Army. (2019). *Field Manual 6-02: Signal support to operations*. Headquarters, Department of the Army.

Burden of Leadership

What the Profession of Arms Requires of Leaders

Lt. Col. Terrance "TP" Pitts
University of Portland Army ROTC

Leadership in the Army's profession of arms is not a reward; it is a debt.

Field Manual 1, the Army's primer on our profession, makes this plain through the actions of Lt. Col. Hal Moore and Sgt. Maj. Basil Plumley at the Battle of Ia Drang. Neither man treated rank as a privilege. Both treated it as an obligation to the Soldiers who depended on them (Department of the Army [DA], 2025, pp. 16–17). That obligation, carried forward across every generation of Army leaders, is the burden this article addresses.

Too many people in positions of authority treat leadership as a title to be worn rather than a weight to be carried. I want to challenge that assumption directly, using FM 1's own description of what our profession requires and pairing it with lessons I have carried from 28 years in uniform.

Force of Will and Weight of Presence

FM 1 states that leaders must possess an indefatigable force of will, and that they must be present with their people rather than managing them from a distance (DA, 2025, pp. 16–17). Moore and Plumley did not lead the 7th Cavalry from a rear command post. They stood in the fight, assessed it in real time, and drove their Soldiers toward success because they refused to let the moment defeat them. That kind of presence costs something. It is far easier to send a message than to stand beside someone in a hard moment, and it is far easier to manage a group chat than to manage a person.

I have said before that there is an equal amount of people watching us in the workplace as there is in a shopping mall or a neighborhood park (Pitts, 2018a). We rarely act like we believe that. Force of will is not loud; it shows in whether a leader shows up consistently – especially when the moment is inconvenient. People watch character, not reputation. Reputation is what we say about ourselves. Character is what we do when we think no one is measuring us against it.

Leading Talent Instead of Fearing It

Few moments test a leader more than the moment an organization produces someone who significantly outperforms their peers. Some leaders respond to talent with insecurity. They begin to micromanage a person they should be developing, and they let their own vulnerability about job security bleed into how they treat their best people (Pitts, 2018b). I believe that response is a failure of leadership, not a symptom of high standards. A leader who needs to be indispensable has stopped leading and started protecting a title.

A better approach follows directly from what FM 1 asks of us: Build an emotional connection with your strongest performers so you can push their skills further rather than contain them.

Create healthy competition that sharpens the whole team rather than just the top performer. Train your replacement deliberately and treat that as a mark of strength, not a threat. Be a change agent who uses talent already inside the organization instead of hoarding the credit. Show humility!

Listen to your people instead of constantly reminding them who is in charge. They already know. They are watching for whether you will use your position for good or simply look out for your best interest.

Leaders who care about the whole person – not just the person's output – build organizations that hold together under pressure.

Loving and Caring for the Whole Person

FM 1 identifies love and care for Soldiers and their families as a defining requirement of Army leadership. It notes that Moore and Plumley earned the loyalty of their unit not simply by driving toward the mission, but by genuinely caring what happened to the people carrying it out (DA, 2025, pp. 16–17). That distinction matters more than most leadership training gives it credit for.

I have watched too many people who call themselves leaders fail to invest in the success of the very people producing results for them. They show no empathy for what a Soldier or civilian employee might be carrying, no real concern for that person's family, and no genuine effort toward their long-term growth (Pitts, 2018a). I still believe in servant leadership – even while I adjust how I lead based on the situation in front of me – because the alternative treats people as "useful" instruments rather than the reason a

mission succeeds in the first place. Leaders who care about the whole person – not just the person's output – build organizations that hold together under pressure.

Building Leaders Who Replace You

FM 1's final requirement is one most leaders resist without realizing it: Leaders are required to make new experts and new leaders, investing deliberately in the next generation – even as people move on, change positions, or leave the organization altogether (DA, 2025, pp. 16–17). This is how the Army remains capable against continuously evolving threats. It is also how an organization outlasts the person currently running it.

I challenge every leader reading this to seek out someone worth bringing along – right now – rather than wait for a formal program to assign one to them (Pitts, 2018a, 2018b). Develop your replacement on purpose. Build well-rounded leaders instead of narrow specialists. Embrace feedback from the bottom-up rather than merely push guidance down. Learn the human dimension and connect with whoever you lead. Build a culture with enough positive energy that people want to stay. We owe a debt of gratitude to those who positioned us for our success – and the only honest way to repay it is to do the same for someone else.

The Weight We Choose to Carry

Leadership in our profession of arms was never meant to be comfortable. FM 1 grounds that truth in Moore and Plumley's example: force of will, presence, genuine care for people and their families, and a deliberate investment in the next generation of leaders (DA, 2025, pp. 16–17). None of those four requirements are optional, and none of them are easy. They are the burden that comes with the title. Carrying that burden well – rather than avoiding it – is what separates a leader followed out of respect from one followed merely out of compliance.

I do not think we should try to make leadership lighter. We must be honest about its weight and choose to carry it anyway, because the people depending on us are worth the cost.

About the Author



Born in Lake Providence, Louisiana, and raised in Las Vegas, Nevada, Lt. Col. Terrance Pitts began his Army career in 1998, rising to the rank of sergeant first class before commissioning as a second lieutenant through Officer Candidate School. He is currently serving as a professor of military science at the University of Portland Army ROTC. Throughout his career, Pitts has served in critical roles across the Army as a communications officer in the U.S. Army Signal Corps with dual master's degrees in human resources development and information technology management from Webster University. His career spans both conventional and special operations units, including two deployments to Iraq. Pitts is currently pursuing a secondary career as an executive coach, trainer, and speaker.

References

Department of the Army. (2025, May 1). The Army: A primer to our profession of arms (FM 1). https://armypubs.army.mil/epubs/dr_pubs/dr_a/arn43687-fm_1-000-web-2.pdf

Pitts, T. (2018a, December 21). Leadership: Beyond the Accolades and Attaboys. LinkedIn. https://www.linkedin.com/pulse/leadership-beyond-accolades-attaboys-terrance-pitts/

Pitts, T. (2018b, December 30). Leadership: Managing Talent vs Being Intimidated. LinkedIn. https://www.linkedin.com/pulse/leadership-managing-talent-vs-being-intimidated-terrance-pitts/



DISA as a Service Member

The Backbone of Modern Battlespace

Sgt. 1st Class Preston W. LaRue
Defense Information Systems Agency

I arrived at the Defense Information Systems Agency (DISA) from an expeditionary signal battalion – where the focus was entirely tactical. As a satellite communication systems specialist (25S), I had little visibility into the strategic reach of the networks and services provided by DISA. However, my experiences and discoveries at DISA have fundamentally changed how I think about military communications and national security.

In modern battlespace, information systems and their data are as critical as ammunition. Behind every successful airstrike, naval maneuver, and ground offensive is a resilient, global network that enables multidomain command and control (C2) – a network entirely delivered, operated, and defended by DISA as a combat support agency.

A typical communications or IT assignment often centers on the tactical edge: making sure a brigade, ship, or squadron has the connectivity to fight and win. While that mission is undeniably vital, it represents only one piece of a much larger puzzle.

A tour at DISA shifts your perspective from the tactical fight to the global enterprise. It exposes you to enterprise-level architecture, policy, and operations that enable forces worldwide. For a service member, this transition means gaining crucial strategic context. You learn how a multitude of highly complex systems integrate across the Department of War Information Network (DoWIN) and see firsthand how those systems support national security at massive scale. It is a profound career multiplier, highly valued by selection boards and senior leaders.

Operating such an expansive global enterprise requires a truly integrated, cross-functional effort. DISA is a joint, interagency environment where Soldiers, Sailors, Airmen, Marines, Guardians,

and civilian professionals work together. Military personnel bring recent tactical experience, operational urgency, and direct liaison capabilities to combatant commands. In tandem, civilian engineers, architects, and program managers contribute institutional knowledge, technical depth, and long-term continuity. Supported by contractors and industry partners who deliver specialized capabilities, they form cohesive teams that design, field, and sustain global cyber operations.

Daily mission success relies entirely on this continuous collaboration. Operators coordinate directly with civilian network engineers to route traffic efficiently, cyber defenders partner with military intelligence to prioritize active threats, and program offices synchronize vital upgrades with warfighter timelines. This cross-pollination accelerates problem-solving and ensures every solution remains operationally relevant.

Because the global battlespace is always active, this integrated mission does not stop for weekends or federal holidays. The agency maintains constant operations to ensure the War Department always has secure, reliable communications. This "always on" continuity is achieved through meticulously planned shift work, rotating watch teams, and redundant staffing models blending military and civilian experts. Standardized handoffs and comprehensive documentation ensure that incoming shifts can pick up operations seamlessly, while comprehensive contingency plans ensure rapid scaling of expert support during crises or critical mission events.

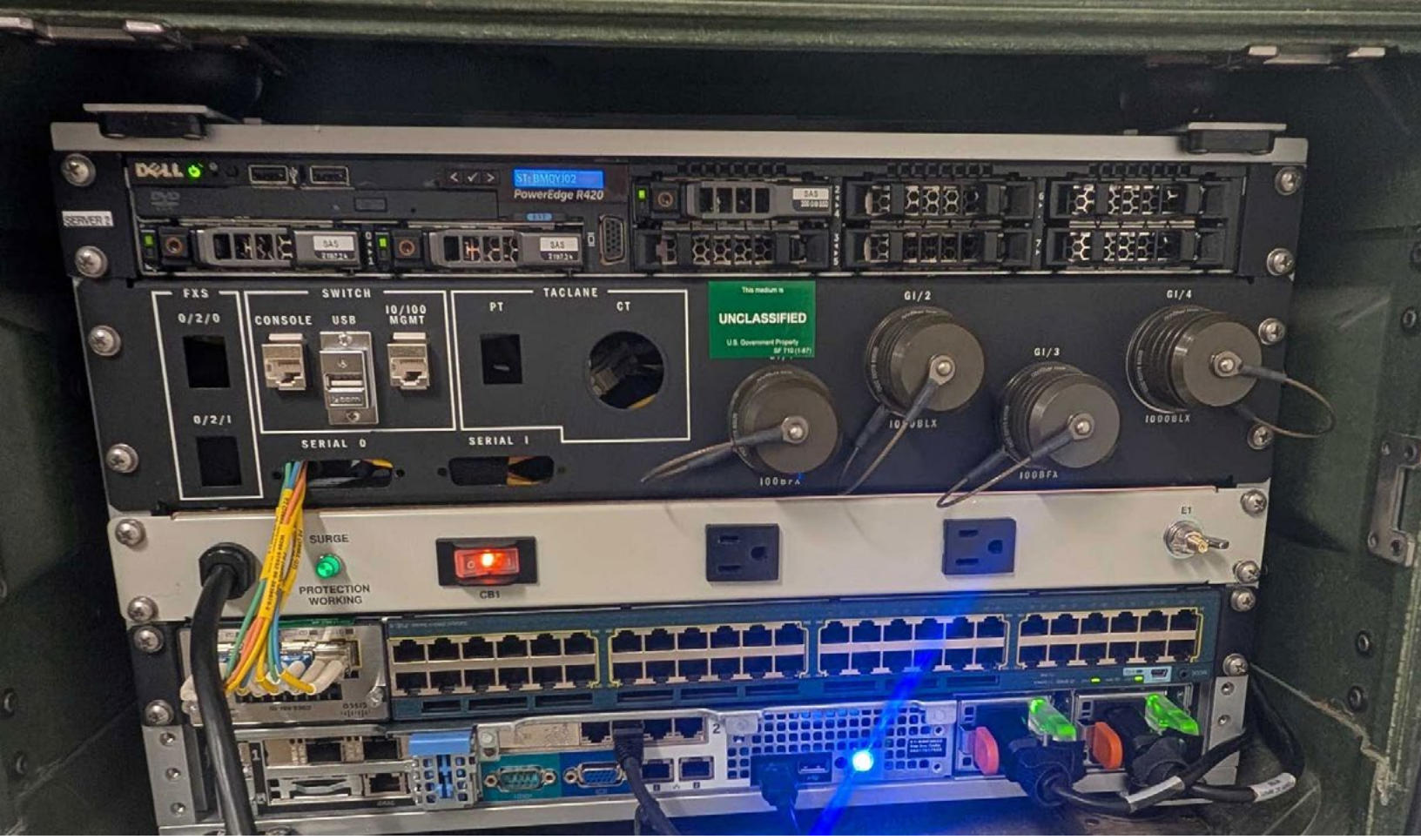
Consider a midnight network outage: It might be detected by a civilian network operations analyst, escalated to a military communications officer assessing the operational impact, and quickly resolved by a joint team coordinating across multiple time zones. This integrated response model is the norm, not the exception.

Ultimately, a DISA tour is far more than a standard shore or staff assignment. It offers unparalleled exposure to joint operations, enterprise cyber defense, complex acquisition processes, and cutting-edge technologies. By working shoulder-to-shoulder with deep technical experts, you learn to translate tactical needs into enterprise-wide solutions, gaining a broader perspective on how the War Department networks support global operations. These enhanced technical and programmatic skills translate directly to future assignments and will strengthen your resume and leadership profile.

About the Author

Sgt. 1st Class Preston W. LaRue enlisted in the Army in December 2009, as an intelligence analyst (35F) and later went on to change his military occupational specialty to satellite communications operator and maintainer (25S). He is currently serving in a nominative assignment as a technical analyst and primary customer liaison for combatant commands under the Defense Information Systems Agency. LaRue's deployments include two combat tours supporting Operation Inherent Reserve along with a deployment to Poland and Germany in support of Operation Atlantic Resolve.





Breaking the Box

Self-Modernizing WIN-T Stacks to Fight Tomorrow's Wars

Col. Kurt W. Page and Capt. Noah R. Ogrydziak
88th Reserve Division and 359th Theater Tactical Signal Brigade

Author's note: *Correspondence concerning this article should be addressed to Col. Kurt Page at: kurt.w.page.mil@army.mil. The views expressed are those of the authors and do not necessarily reflect the official policy or position of the Department of the Army, the Department of War, or the U.S. government.*

U.S. Army Reserve signal brigades are a vital enabler of the Army's total force communications architecture. Signal units provide the backbone for command and control, mission command applications, and joint interoperability, while playing a critical role in enabling communications for distributed, expeditionary, and large-scale combat operations (LSCO).

As warfare becomes increasingly contested across land, cyber, and space domains, reliable communications are essential for both Reserve and active-duty Army components; yet the Reserve faces a unique modernization dilemma.

While active-duty formations receive newer, integrated systems on accelerated fielding timelines, Reserve units often continue to operate legacy platforms for extended lifecycles. Warfighter Information Network-Tactical (WIN-T) is one example. It has served nearly two decades as the Army's principal upper-tier tactical internet, linking battalion-through-corps formations to the Department of War Information Network (Department of the Army, 2016).

WIN-T and Tactical Server Infrastructure hardware are being divested—and replaced with NGC2-capable transport, infrastructure, data,

A detailed view highlighting the front (NIPR) configurations of the modified Joint Network Node-Enhanced (JNN-E) at the Army Reserve Center, Fort Gordon, Georgia. While a standard fielded JNN system is housed in a large, vehicle-mounted shelter, 359th Theater Tactical Signal Brigade Soldiers utilized virtualization techniques to condense the entire suite of baseband equipment into a single, highly portable transit case. ***(U.S. Army photo by Capt. Noah Ogrydziak)***



Soldiers assigned to 392nd Expeditionary Signal Battalion showcase a Starshield terminal during a Combat Support Training Exercise at Camp Shelby, Mississippi, June 2026. This cutting-edge equipment serves as the primary network transport system for all 359th Theater Tactical Signal Brigade tactical nodes, delivering reliable NIPR and SIPR communications. ***(Courtesy photo)***

and application-layer hardware—across all three components, at the fastest pace in Army history under the Army G-6's Command and Control Network Optimized for Warfighting (C2NOW) initiative: a 30-month acceleration effort and the Army's stated on-ramp to Next Generation Command and Control (NGC2). Yet it remains the foundation of Reserve communications—and without adaptation, it risks becoming a liability in future operations.

Regional fielding is set to begin fiscal year (FY) 2026 with a goal of transforming the Army's tactical network baseline by 2029 (Capability Program Executive Command and Control Information Network, n.d.; Pomerleau, 2026). The FY27 budget request alone commits roughly $3.7 billion to NGC2 and C2NOW, including more than $500 million earmarked specifically to replace fielded WIN-T transport equipment (Janes, 2026; Office of the Assistant Secretary of the Army [Financial Management & Comptroller], 2026).

Under the Army's regional fielding construct, Reserve signal brigades face a multiyear capability gap due to the Army prioritizing active-duty equipment fielding. They will retain WIN-T equipment the Army has begun divesting elsewhere while NGC2-capable transport is issued to active-duty formations first. All three components conduct New Equipment Training at shared regional sites, but the Army National Guard (COMPO 2) and Army Reserve (COMPO 3) equipment is shipped to home station. Historically, this sequencing has left the Army Reserve absorbing legacy risk the longest.

Recent Reserve equipping data show that roughly one-third of Reserve mounted command-and-control systems were not network capable, against a multibillion-dollar equipping shortfall relative to active-duty Army (Department of Defense, 2019). Left unaddressed, that same sequencing risk applies to C2NOW. Reserve signal formations could face a multiyear capability trough, still holding WIN-T equipment the Army has already begun to divest elsewhere while NGC2-capable replacement transport is fielded to active-duty Army formations first.

This article argues that approximately 155 end-of-life WIN-T systems already on hand should be collapsed and virtualized into a smaller number of consolidated, software-defined nodes, augmented by proliferated low Earth orbit (pLEO) satellite communications (SATCOM), 5G tactical cellular, and commercial cloud backhaul. This hybrid approach converts a sunk, depreciating asset—part of a WIN-T Increment 2 program representing a $20 billion total lifecycle investment (Office of the Secretary of Defense, 2018)—into a bridge capability that delivers four concrete outcomes for the command.

Bridge the Gap to C2NOW

By keeping a functioning upper-tier tactical internet (Upper TI) in the fight throughout the Army's 30-month C2NOW sprint, the brigade avoids a communications trough while its formations wait in the COMPO 2/3 fielding queue. Soldiers, staff, and mission command systems stay networked on a modernized WIN-T backbone until NGC2-capable transport and infrastructure hardware is issued to the Reserve, not merely programmed for it.

Increase Training and Skill Development

Virtualization, server-stack consolidation, and software-defined transport are the same disciplines NGC2's infrastructure and transport layers will demand at scale (U.S. Army, 2026). By training now on collapsed, virtualized WIN-T stacks, signal Soldiers build hands-on proficiency in cloud-to-edge computing, network orchestration, and systems administration. This will shorten the brigade's future NGC2 adoption timeline and give part-time Soldiers a direct bridge between weekend training, civilian information technology (IT) certifications, and future mission command systems.

Fielding Upper TI Nodes to Brigade and Above

Collapsing multiple WIN-T Upper TI node functions onto fewer virtualized platforms frees excess hardware from the existing 155-system inventory for redistribution, extending functioning Upper TI connectivity to brigade, division, and echelons-above-brigade formations that would otherwise wait

for new C2NOW-T procurement to reach them. This reuses capital the Army has already purchased rather than require new transport buys. Furthermore, it can largely execute via existing organic lift and scheduled fielding events rather than by dedicated transport or logistics campaign.

A More Robust, Survivable, Redundant Network

Distributing a larger population of lower-cost, virtualized legacy nodes—rather than concentrating capability in a smaller number of high-value C2NOW replacement systems—adds path and hardware diversity to the tactical network. This complements incoming NGC2 transport. This redundancy is both a hedge and a capability: Congressional signals point to possible reductions to the FY27 C2 Transport and C2 Infrastructure budget lines (Minadeo, 2026), and NGC2 fielding beyond the initial 4th Infantry Division and 25th Infantry Division prototypes is still being scaled unevenly across the force (Harper, 2026). A Reserve network that does not depend entirely on the pace of NGC2 fielding is more survivable, regardless of how quickly the rest of the Army converts.

Together, these four outcomes turn on-hand WIN-T equipment into a readiness asset rather than a liability, sustaining Reserve formations while building the technical bench strength those same Soldiers will need for future NGC2 arrival.

Legacy Capabilities and Current Gaps

Designed to connect tactical formations at battalion through corps levels, WIN-T provides satellite, line-of-sight, and mission command capabilities (Department of the Army, 2016). It brought significant advances in bandwidth and mobility compared with earlier systems.

Limitations

Mobility. WIN-T Increment 2 nodes are bulky, vehicle-mounted, and less agile than current expeditionary systems.

Complexity. Multiple servers, enclaves, and hardware stacks create sustainment and training burdens.

Cybersecurity. Legacy baselines were not designed with modern zero-trust or endpoint security requirements.

Integration. Bridging joint and coalition networks or incorporating commercial transport solutions is difficult.

For Reserve formations, these limitations manifest as slower deployment timelines, larger sustainment burdens, and risk of falling behind the pace of modern operations. To mitigate these gaps, Reserve signal brigades are adopting a pragmatic modernization strategy.

Modernization Approach: Virtualization and Stack Consolidation

Collapsing Server Stacks. By consolidating multiple legacy hardware servers into virtualized environments, units reduce physical footprint while retaining required services. This enables a single piece of hardware to host multiple mission-critical applications.

Leveraging Virtual Servers and Applications. Virtualization enables rapid provisioning, cloning, and resource reallocation. Instead of transporting redundant hardware, units can load multiple instances on fewer devices.

Transport Layer Evolution. While WIN-T provides the backbone, newer technologies such as pLEO satellites, 5G tactical cellular, and cloud backhaul can be integrated. This hybrid transport approach increases resiliency and flexibility.

Cybersecurity Adaptation. Virtualization facilitates tighter monitoring, patching, and baseline control, providing Reserve units a way to elevate cybersecurity posture without full equipment replacement.

This approach keeps WIN-T relevant while gradually integrating future Integrated Tactical Network (ITN) capabilities.

Operational Advantages

The shift toward virtualization offers tangible operational benefits.

Reduced Size, Weight, and Power. Lighter server stacks and fewer hardware boxes ease mobility burden, which is critical for Reserve units deploying from dispersed locations.

Improved Interoperability. Virtual environments align better with enterprise IT architecture, simplifying integration with active-duty, joint, and coalition networks.

Faster Deployment. Prebuilt virtual images reduce services' configuration times from days to hours.

Training Alignment. Because many civilian IT enterprises rely on virtualization, Reserve Soldiers gain transferable skills that enhance readiness both in military and civilian careers.

Implementation in Reserve Context

Unlike active-duty units, Reserve formations operate under constrained budgets and limited training time. Virtualization directly addresses these constraints.

Pilot Programs. Several Reserve signal formations are experimenting with collapsing mission command applications onto single virtualized

platforms, reducing equipment transported to training exercises.

Integration With Active Component. Reserve units can arrive at large-scale exercises already configured to integrate with division or corps headquarters, reducing interoperability challenges.

Resource Efficiency. Rather than waiting for full ITN fielding, Reserve brigades maximize legacy WIN-T investments while incrementally adopting modern solutions.

Risks and Mitigation Strategies

Adopting a hybrid modernization strategy introduces challenges that must be actively managed.

Technical Risks. Virtualization requires ensuring that legacy hardware can host newer software loads without degradation. Mitigation: phased validation and pre-deployment testing.

Training Gaps. Reserve Soldiers may lack familiarity with virtualization tools. Mitigation: targeted professional military education modules and leveraging civilian-acquired IT certifications.

Sustainment Risks. Legacy WIN-T components may become harder to support. Mitigation: building sustainment partnerships and using virtualization to minimize dependence on older hardware.

Outlook

This hybrid model maximizes legacy equipment while integrating modern virtualization and positions the Reserve for a smoother transition to the Army's ITN. Virtualized environments will dovetail with future cloud-based tactical systems, software-defined radios, and artificial-intelligence-enabled cyber defense capabilities.

Over the next decade, Reserve units will both sustain communications capabilities and integrate modernization directly into training. By combining operational readiness with hands-on exposure to emerging systems, Reserve Soldiers can validate and adapt new technologies in a part-time force context. This dual focus keeps the Reserve current with evolving capabilities, accelerates technology integration, and provides a force that is both adaptive and cost-efficient to the Total Army, while keeping pace with rapid technological change.

Recommendations

Incremental Modernization. Prioritize virtualization to extend WIN-T relevance while preparing for ITN.

Training Pipelines. Incorporate virtualization and cloud fundamentals into Reserve signal military occupational specialty training.

Industry Partnerships. Explore commercial off-the-shelf virtualization and transport solutions for rapid adaptation.

Reserve-Led Proof of Concept. Establish pilot brigades as innovation hubs to test virtualization at scale.

Conclusion

Reserve signal brigades are confronting a dual challenge: sustaining legacy WIN-T systems while driving forward into the next era of network modernization. Rather than treat this as a constraint, brigades are converting it into a strategic advantage. By collapsing server stacks, expanding virtualized infrastructure usage, and integrating emerging transport technologies, formations are transforming a complex requirement into a cost-neutral readiness accelerator.

This modernization-through-adaptation approach ensures the Reserve remains a relevant, reliable, and agile communications force capable of bridging legacy architecture with future tactical network environments. Signal brigades are not merely maintaining the network; they are reshaping it to expand commander decision space, strengthen operational flexibility, and deliver a more resilient communications posture for the force.

About the Authors

Col. Kurt W. Page began his military career enlisting as an infantryman in the Army. In 1994, he commissioned as an infantry officer and distinguished military graduate upon completing Officer Candidate School at Fort Benning, Georgia. Page earned his undergraduate degree in computer engineering from Columbus State University and completed a master's degree in leadership and management in 2018. He is a resident graduate of the U.S. Army War College, where he served as a cyber fellow at University of Pittsburgh and Carnegie Mellon University. Page has led at brigade, battalion, company, and platoon levels, having served in a wide range of key developmental and strategic positions. He is currently assigned as the chief of staff for the 88th Reserve Division at Fort McCoy, Wisconsin.

Capt. Noah R. Ogrydziak commissioned as an active-duty Army signal officer upon graduating from the United States Military Academy in 2017 with a Bachelor of Science in computer science. A graduate of the Army's Functional Area 26A (Network Systems Engineer) course, Ogrydziak has served at battalion and brigade levels as a network operations officer, technical instructor, and network engineer. While serving as the network engineer for 307th Expeditionary Signal Battalion (ESB), he spearheaded the unit's modernization and transition to an ESB-Enhanced (ESB-E), directing the tactical integration and fielding of Scalable Network Nodes. Ogrydziak is currently pursuing a Master of Science in network engineering at the University of Colorado Boulder, with an expected graduation in 2027.

References

Capability Program Executive Command and Control Information Network. (n.d.). Today's #WorkforceWednesday highlights the Command and Control Network Optimized for Warfighting (C2NOW) team [Post]. Facebook. https://www.facebook.com/cpec2in/posts/todays-workforcewednesday-highlights-the-command-and-control-network-optimized-f/1347217314105935/

Department of Defense. (2019). National Guard and Reserve equipment report for fiscal year 2019 (NGRER FY2019). https://prhome.war.gov/portals/52/documents/pr%20docs/ngrer%20fy2019.pdf

Department of the Army. (2016). Techniques for Warfighter Information Network–Tactical (Army Techniques Publication 6-02.60). https://www.bits.de/nraneu/others/amd-us-archive/atp6-02-60(16).pdf

Harper, J. (2026, July 31). "Ready, but not done": The Army will start scaling parts of its NGC2 to more units. DefenseScoop. https://defensescoop.com/2026/07/31/army-ngc2-start-scaling-parts-to-more-units/

Janes. (2026, April 22). Pentagon budget 2027: US Army requests over USD3 billion for NGC2, C2NOW. https://www.janes.com/defence-intelligence-insights/defence-news/c4isr/pentagon-budget-2027-us-army-requests-over-usd3-billion-for-ngc2-c2now

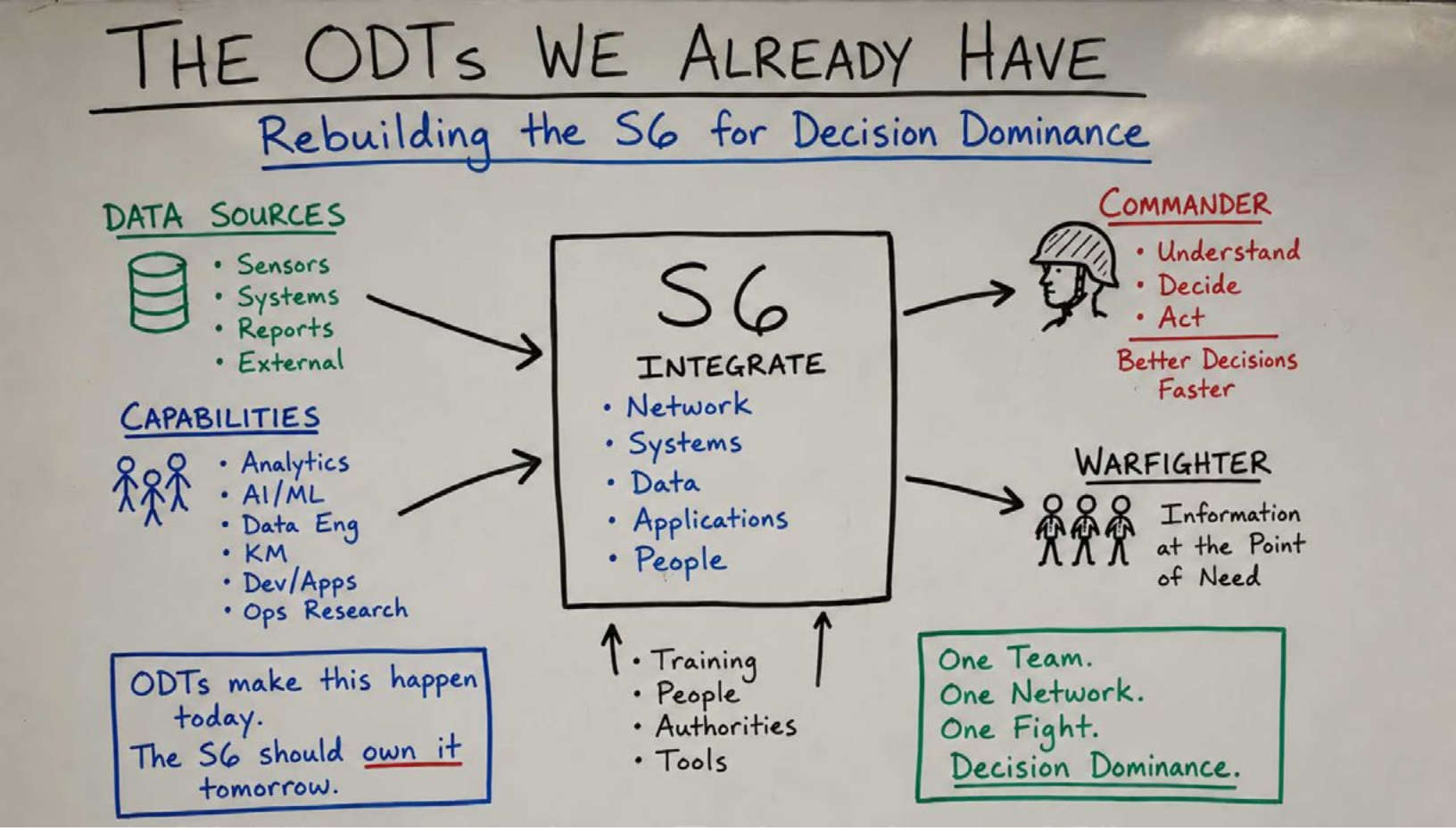
Minadeo, D. (2026, July 6). Army, Anduril work out common data layer baseline for NGC2. Inside Defense. https://insidedefense.com/insider/army-anduril-work-out-common-data-layer-baseline-ngc2

Office of the Assistant Secretary of the Army (Financial Management & Comptroller). (2026). Other procurement, Army: Budget activity 2: Communications and electronics (Fiscal year 2027 budget estimates). https://www.asafm.army.mil/portals/72/documents/budgetmaterial/2027/discretionary%20budget/procurement/other_procurement%20-%20ba2%20-%20communications%20%26%20electronics.pdf

Office of the Secretary of Defense. (2018, December). Warfighter Information Network–Tactical Increment 2 selected acquisition report. https://www.esd.whs.mil/portals/54/documents/foid/reading%20room/selected_acquisition_reports/fy_2018_sars/19-f-1098_doc_87_win-t_inc_2_sar_dec_2018.pdf

Pomerleau, M. (2026, February 4). Army plans for division to receive NGC2 production ecosystem in FY27. Breaking Defense. https://breakingdefense.com/2026/02/army-plans-for-division-to-receive-ngc2-production-ecosystem-in-fy27/

U.S. Army. (2026, January 29). NGC2: Data-informed sustainment decision making. https://www.army.mil/article/290029/ngc2_data_informed_sustainment_decision_making



Rebuilding S6 for Decision Dominance

Maj. Aaron S. Fernandez
U.S. Army Signal School

"The stack is down."

That phrase has become convenient shorthand in technical formations, but shorthand is not a diagnosis. Is the router reachable? Did a switch lose its uplink? Is the server unavailable? Is the application failing? What changed? What troubleshooting has already been done? What do we actually know before saying "the stack is down?"

These questions should be routine in a technical profession. Yet across Signal formations, we use vague language such as "stack," "box," and "system," when we should be naming the actual technology. Language matters. If we cannot accurately describe our systems to one another, we should not be surprised when we struggle to troubleshoot, integrate, or explain them to commanders (Gandy, 2026). At the same time, the Army is moving toward data-centric operations, artificial intelligence (AI), machine learning (ML), and increasingly interconnected command and control (C2) systems. Operational data teams (ODTs) have emerged to help turn data into information commanders can use. The requirement is real, and these teams are addressing real operational problems. Current Army modernization efforts increasingly describe C2 as integrating transport, data, software, and infrastructure to support faster, better decisions (Adkins, 2025; Office of the Chief Information Officer [OCIO], 2022; U.S. Army, 2026).

Before making an ad hoc solution permanent, the Signal Corps should ask a harder question: Are we building another technical staff because we have not properly trained, employed, and resourced the one we have?

If the Army seeks decision dominance, it should be cautious about creating new seams between the network, data, applications, and the commander. Rather than build another S6 beside the S6, the Army should determine whether the better response is to train, organize, and resource the S6/G6 to serve as the commander's principal technical integration staff.

Speak Like a Technical Professional

Signal professionals must translate technical complexity for commanders. A maneuver commander should not need a networking certification to understand how a problem affects the

The author used artificial intelligence to generate this diagram, which mimics his style of whiteboarding

fight. That is our job. Translating outward should not require imprecision inward.

Doctors use medical terminology with doctors. Pilots use aviation terminology with pilots. Engineers use engineering terminology and translate it for others. The Signal Corps should do the same. Precision should be expected. A router is a router. A switch is a switch. A server is a server. Transport, applications, identity services, storage, and compute are not interchangeable terms; those distinctions matter.

"The stack is down" should be a conversation starter, not a diagnosis. When a signal professional reports a problem, the discussion should quickly move past "it is down." What failed? What has been checked? What changed? What help is needed? Officers and senior noncommissioned officers do not need to solve every problem themselves, but they should know enough to ask the next technical question. A signal leader does not need to be the deepest expert in the room – but they should be technically competent enough to understand it (Gandy, 2026).

This is more than a matter of vocabulary. Precision in language reflects precision in thought, and precision in thought is foundational to troubleshooting, planning, integration, and C2.

Stop Wasting Technical Talent

The Army invests heavily in technically specialized officers, warrant officers, and NCOs. Too often, however, signal professionals are placed in positions that limit use of the expertise the Army spent years developing. Rarely is there a single reason. Good technical people become known as problem-solvers, so headquarters use them outside their specialties. Some officers may believe broader assignments improve evaluation reports or promotion prospects. Sometimes units are simply undermanned. Each decision may make sense in isolation. Over time, however, those decisions erode the Signal Regiment's technical depth. Broadening has value, but it should not replace deliberate technical talent management. A technical branch should be disciplined about where it employs scarce technical expertise.

The Army also needs to examine incentives. If technical officers conclude that leaving technical work is the path to advancement, expertise will atrophy. If warrant officers and technical NCOs become general-purpose staff talent because they are dependable, formations will eventually lose the deep technical leadership they require. If the Army says technical expertise matters, talent management practices should reflect that judgment. Signal professionals must be trained technically, employed technically, developed continuously, and given enough time in technically relevant assignments to remain credible (Christensen & Sack, 2026; Newkirk, 2026).

ODTs Solve a Real Problem

Commanders increasingly need data from disparate systems collected, transported, transformed, analyzed, and delivered quickly enough to influence decisions. AI and machine learning will only increase that demand. The tactical network now connects sensors, applications, data, computing resources, algorithms, and decision-makers. That environment cannot be understood solely as transport (Adkins, 2025; OCIO, 2022).

It is easy to understand why ODTs emerged. There is a real gap, and existing staff have not always delivered the data capability commanders need. A cross-functional team makes sense. Signal neither possesses nor should attempt to recreate every specialty required for data-enabled decision-making (Adkins, 2025). The Army already recognizes the problem at scale. The recently launched Army Data Operations Center reflects a real institutional requirement for authoritative data access, brokering, and connectivity across the force. However, this development does not answer the tactical and operational questions of who integrates transport, applications, services, and data flows at echelon for commanders operating in contested environments (U.S. Army, 2026). That should concern the Signal Corps.

If the requirement is enduring, should the Army automatically convert the ad hoc team into another enduring organization? Or should it first ask why the existing technical staff lacks organization and resources to integrate those capabilities for the commander? Any ODT depends on technical infrastructure that someone must design, secure, sustain, and integrate. Data must move. Applications must run. Compute and storage must exist somewhere. Users must authenticate. Systems must communicate across contested, intermittent, and bandwidth-constrained environments. All of that depends on a technical architecture that someone at echelon must integrate for the commander.

Don't Build Another S6, Build a Better S6

ODTs address a real capability gap, but an effective ad hoc solution can quickly become the default answer. Before that happens, the Army should ask if it is creating a new organization merely to compensate for an under-resourced one. For commander-facing technical integration at echelon, that organization should be the S6/G6. This does not mean every ODT member should be a signal Soldier.

Operations research, intelligence, software development, knowledge management, data science, and other specialties contribute expertise the Signal

Corps should integrate rather than duplicate (Adkins, 2025; Millare & Donathan, 2025). A better option is to augment a properly trained and resourced Signal staff for integrating the technical environment through which data becomes operationally useful. If Signal's responsibility ends once packets cross the network, then data orchestration may belong elsewhere. If Signal provides the technical environment that enables C2, transport cannot be neatly separated from the applications, services, compute, identity, and data flows that make that environment useful.

The modern S6 should be more than the helpdesk commanders call when communications stop working. It should be the commander's principal technical integration staff at echelon. Rebuilding the S6 will also require targeted growth in technical competencies across the Signal workforce. That does not mean turning every data network engineering officer (FA26) or signal warrant officer into a data scientist or software engineer. It does mean giving network systems engineers (26As), data systems engineers (26B), data operations warrant officers (255A), network operations warrant officers (255N), and cyber defense warrant officers (255S) greater literacy in data architectures, automation, cloud-enabled services, API-enabled integration, AI/ML-enabled decision support tools, and the security and sustainment requirements that accompany them. If these professionals are expected to integrate the technical environment at echelon, they must understand not only how data moves, but how modern services, platforms, and analytic tools depend on – and interact with – the network (Millare & Donathan, 2025).

This is not an argument for Signal ownership of every algorithm, platform, or dataset. It is an argument that the Army must not solve an integration problem by creating another boundary across which integration must occur.

Decision Dominance Requires Integration

This is not about protecting Signal turf. If an ODT produces a better operational outcome, commanders should use it. The question is whether another enduring technical organization is the best way to achieve the speed and integration the Army wants.

Decision dominance requires sensors, networks, data, applications, analytics, AI, and commanders to function as an integrated system. Army modernization commentary recognizes that signal formations must evolve beyond a transport-only mission if they are to support Next Generation Command and Control (NGC2) and data-enabled C2 at scale (Millare & Donathan, 2025; U.S. Army, 2026).

Organizational design can support that integration – or hinder it. Every additional staff boundary creates another handoff. While some are necessary, others are self-inflicted and unnecessary. If one organization owns transport, another owns data access, another develops software, another conducts analytics, and another integrates the result for the commander, requirements and information must cross each of those boundaries. The Army can easily create organizational latency while trying to eliminate technical latency. That is the tension worth examining as the Army pursues decision dominance. Are its organizations helping technology integrate? Or are they adding another layer between the commanders and technology?

ODTs have exposed a legitimate requirement. The enduring lesson may be less about creating another permanent team and more about recognizing what the S6/G6 and the Signal Corps must become.

Conclusion

Evolution begins with culture. Signal professionals should speak precisely to each another and translate clearly for commanders. The Signal Regiment should maintain meaningful technical standards and deliberately employ its trained talent. As emerging technologies increasingly depend on the network, the Signal Corps should examine how it must evolve to integrate them (Christensen & Sack, 2026; Gandy, 2026; Newkirk, 2026).

Signal does not need to own every algorithm, application, or dataset; nor should it attempt to replace Cyber, Space, Software Operations, Operations Research, Intelligence, Knowledge Management, or Data Science. Those communities provide expertise the Army needs. Signal's responsibility is to integrate the technical environment through which those capabilities create effects for commanders.

ODTs have exposed a legitimate capability gap. Before creating another enduring technical organization to fill it, the Army should ask if it has adequately trained, organized, and resourced the S6 already standing beside the commander.

Commanders own the network. The Signal Corps is entrusted to make it work. As the network evolves to include data, applications, automation, and AI-enabled capabilities, that responsibility must evolve with it. The ODT we already have may be the S6 we have not yet modernized.

About the Author

Maj. Aaron S. Fernandez is the FA26A Career Program Manager in the Office of the Chief Signal Officer at Fort Gordon, Georgia, where he previously served as the Functional Area Branch Chief at the U.S. Army Signal School. He commissioned from the United States Military Academy in 2011 and has served in various roles across the U.S. Army.

References

Adkins, A. K. (2025). Achieving decision dominance: The arduous pursuit of operationalized data. Military Review, 105(1). https://www.armyupress.army.mil/journals/military-review/english-edition-archives/january-february-2025/decision-dominance/

Christensen, N., & Sack, W. (2026). Restoring the scholar-warrior: A shared mandate for students, instructors, and the Signal School. Army Communicator. https://www.lineofdeparture.army.mil/journals/army-communicator/archive/summer-2026/restoring-the-scholar-warrior/

Gandy, L. M. (2026, July 23). The enduring Signaleer: Understanding the "why" and "how." Army Communicator. https://www.lineofdeparture.army.mil/journals/army-communicator/archive/summer-2026/the-enduring-signaleer-understanding-the/

Millare, E., & Donathan, R. (2025, November 1). Aligning force structure for NGC2: Decision dominance. Army Communicator. https://www.lineofdeparture.army.mil/journals/army-communicator/archive/fall-winter-2025/aligning-force-structure-for-ngc2/

Newkirk, W. L. (2026). Employing the right technical expert: Why Signal WOs specialization matters. Army Communicator. https://www.lineofdeparture.army.mil/journals/army-communicator/archive/summer-2026/employing-the-right-technical-expert/

Office of the Chief Information Officer. (2022). Army data plan. U.S. Army. https://api.army.mil/e2/c/downloads/2022/10/13/16061cab/army-data-plan-final.pdf

U.S. Army. (2026, April 9). Army launches Data Operations Center to give warfighters the decisive edge. https://www.army.mil/article/291655/army_launches_data_operations_center_to_give_warfighters_the_decisive_edge



Modernizing the CGSC's Wireless Network

A Blueprint for Data-Centric Curriculum

Maj. James Jagozinski and Peter Cerny
Command and General Staff College

The Command and General Staff College (CGSC) established a commercial wireless network (CGSCNet) in 2007 to provide a commercial wireless network for about 1,000 students and dependents at the Fort Leavenworth CGSC campus in Kansas.

Over the past two decades, CGSCNet has evolved to provide a mission-critical capability for over 3,000 students, faculty, and guests attending CGSC. CGSCNet evolved and matured rapidly following the COVID-19 pandemic to support CGSC's shift to a Bring Your Own Device (BYOD) model. Today, that BYOD foundation has allowed CGSC to incorporate commercial and government artificial intelligence (AI) and data-centric platforms into the curriculum. Network transport and managed firewall services are provided by the Kansas Research and Education Network (KanREN), a non-profit organization headquartered at the University of Kansas.

The Problem

CGSCNet suffered from quality-of-service complaints on an almost daily basis prior to September 2025. Beginning in September 2025, the CGSC Academic Support Directorate (ATSD) Network Operations Security Center (NOSC) began a comprehensive analysis to identify root causes of CGSCNet quality of service. Problems included legacy infrastructure, misconfigurations, lack of redundancy,

Department of Army civilians Neal Barnett (left), network administrator, and Peter Cerny, network chief, conduct upgrades to the CGSC wireless network. ***(Photo by Maj. James Jagozinski, CGSC)***

and lack of accurate documentation. These problems compounded leaving a fragile, underperforming network that was incapable of supporting emerging technologies planned to be incorporated into the curriculum for Academic Year (AY) 27.

Solution and Immediate Impact

The ATSD NOSC recognized the threat to the academic mission and immediately developed a stabilization plan to address problems with the existing infrastructure. First, NOSC technicians addressed the wireless local area network (WLAN) controller issue by upgrading WLAN controller hardware and firmware, which increased throughput throughout the network and allowed the ATSD NOSC to establish a high-availability pair for a critical system. Simultaneously, wireless access point (WAP) firmware was also updated to be interoperable with the WLAN controller during this step which increased performance throughout the campus.

Finally, ATSD NOSC identified the boundary firewall was a bottleneck after LAN issues were resolved. ATSD NOSC coordinated with KanREN to replace the CGSCNet boundary firewall to allow our full 1 Gbps backbone to operate at capacity. KanREN replaced the firewall within one week – something that would not be feasible using Army procurement processes. These decisive actions restored reliability and drastically improved performance.

Way Ahead: Modernization and Capability

In February 2026, the CGSC commandant initiated a Professional Military Education (PME) Modernization program. One goal of the PME Modernization effort was to integrate AI and data-centric capabilities into the AY27 curriculum. The ATSD NOSC developed a full network modernization (NETMOD) plan for the CGSCNet to upgrade to a 10 Gbps backbone, deploy WiFi 7-ready access points, and consolidate the network core into the NOSC's secure telecommunications room with redundant power and HVAC. This NETMOD ensures CGSCNet is prepared to handle intensive, data-centric workloads. ATSD initiated procurement for new equipment and installation but received no bids. ATSD rapidly pivoted towards U.S. Army Information Systems Engineering Command (ISEC) for assistance with the procurement and installation to meet our Nov. 1, 2026, deadline.

Key Takeaways

BYOD and AVD are force multipliers. Leveraging BYOD/AVD and providing a robust commercial network minimize overhead costs while delivering superior performance for commercial, cloud-based tools used in modern training.

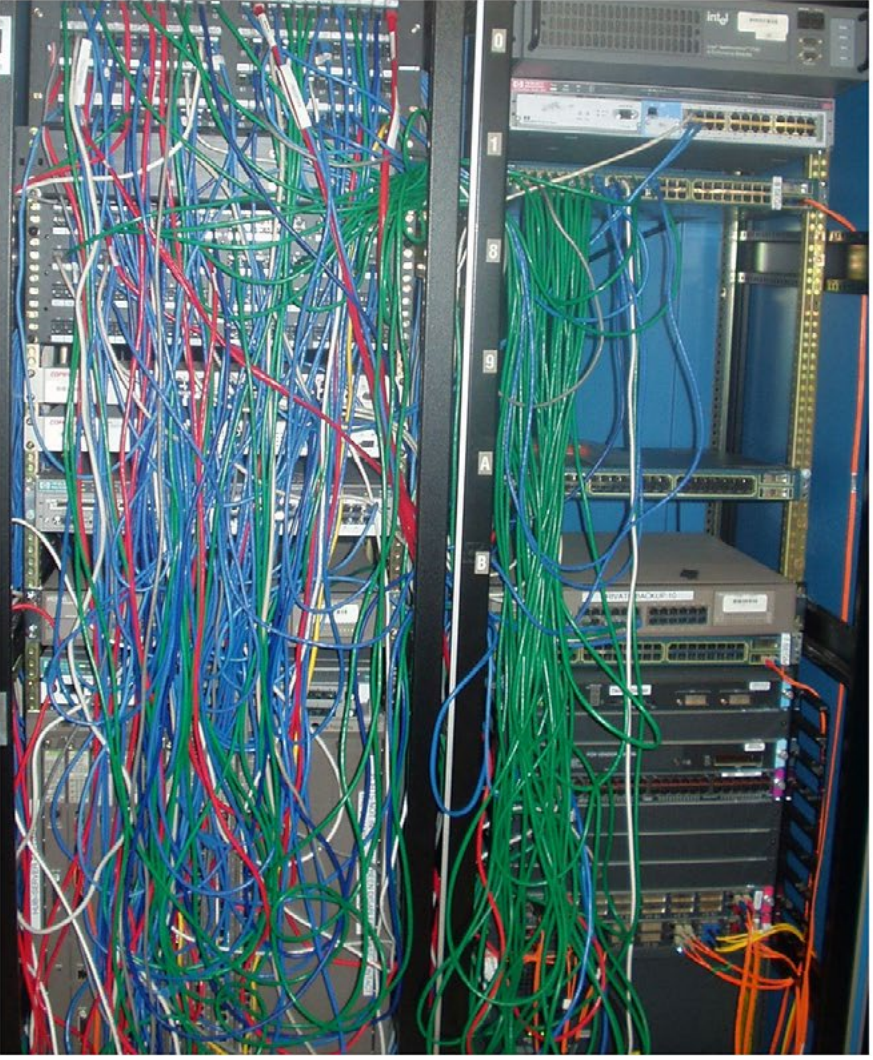
Network lifecycles are non-negotiable. Organizations must consistently fund network lifecycles to prevent reliance on legacy equipment. AI and data platforms are useless if the network is neglected.

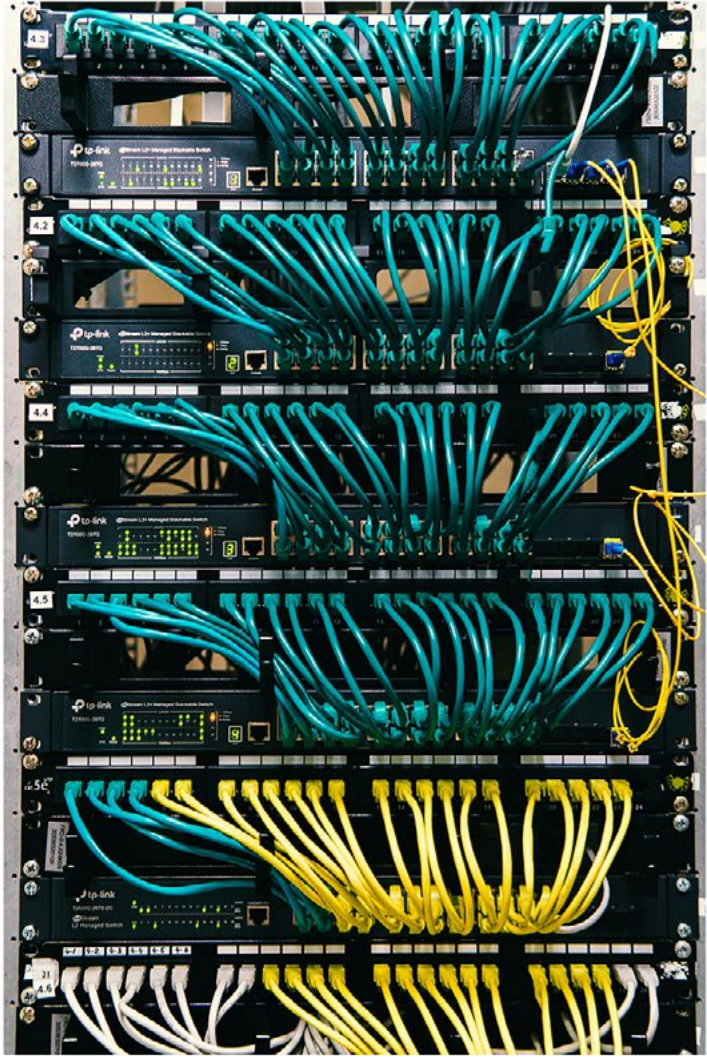
Cultivate vendor partnerships. Third-party vendors with service contracts are invaluable, especially when the relationship is treated as a strategic partnership rather than a transactional customer-vendor exchange.

About the Authors

Maj. James "Jimmy" Jagodzinski is the technical director for the Academic Technology Support Directorate (ATSD) at CGSC. He supervises the NOSC, Data and Applications Team, and Cybersecurity sections within ATSD.

Pete Cerny is an IT specialist (network services) and the Network Operations Security Center supervisor for the ATSD at CGSC. He manages a four-person team that is responsible for the installation, operation, and maintenance of a stand-alone network and commercial network, and provides systems administration for Army Enterprise Unclassified Services at CGSC.





Standardizing Military Installation Resilience

From the Foundation to the Firewall

Larry Poole
U.S. Army Information Systems Engineering Command

Note: *Artificial intelligence assistance was utilized in the preparation of this article. Specifically, Gemini Enterprise (Google, 2026) was used for structural refinement and formatting references.*

Picture a modern command post on a U.S. Army installation. Inside, an operations officer monitors a real-time common operational picture, while beneath the floor and behind the drywall, thousands of feet of fiber-optic cabling transport critical tactical data. Above the cabling, smart environmental control systems regulate temperatures, while external security cameras stream high-definition video over internet protocol networks. Historically, heating, cooling, and air conditioning (HVAC) and network systems were viewed as entirely separate entities.

In an era defined by evolving cybersecurity threats and increasingly volatile environmental conditions, a military installation's physical buildings can no longer be viewed as separate from its digital networks. To achieve true mission assurance, the Army must treat its physical plant as a direct extension of its digital network, embedding cybersecurity and technical resilience from the very start of the design and construction process.

As a major subordinate command of U.S. Army Communications-Electronics Command, the U.S.

A side-by-side comparison of non-standardized telecommunications cabling (left) and a standards-compliant cabling installation (right). The stark contrast between these two cabling implementations highlights the necessity of standardized infrastructure. Following unified standards, such as UFC 3-580-01, ensures the armed services consistently utilize the proper materials, methodologies, and quality controls. ***(Left: Photo by Larry Poole, USAISEC; Right: Stock photo via Unsplash.)***

Army Information Systems Engineering Command (USAISEC) plays an enduring role in publishing the vital technical standards that enhance military installation resilience. These standards directly shape the information and communications infrastructure across all branches of the armed forces.

Defining Modern Resilience

To appreciate the scope of this mission, one must look at how the law defines military installation resilience. Title 10 of the United States Code, Section 101, establishes the baseline for military preparedness and environmental adaptability. Under this statute, resilience is defined as the capability of an installation to avoid, prepare for, minimize the effect of, adapt to, and recover from extreme weather, environmental changes, energy or water disruptions, or human-induced hazards (10 U.S.C. § 101, 2021).

For Soldiers operating worldwide, a resilient installation ensures essential logistical, transportation, and communications systems remain operational during a crisis. Maintaining these mission-essential functions requires a holistic engineering approach. USAISEC engineers possess the dual expertise in physical infrastructure and information technology (IT) necessary to bridge these domains. By treating the physical plant as an extension of the digital network and embedding cybersecurity requirements into initial facility designs, USAISEC helps ensure Army bases are inherently robust enough to withstand and recover from modern threats.

Translating Expertise into Universal Standards

USAISEC acts as a primary subject matter expert for joint, discipline-specific working groups, translating specialized engineering expertise into mandatory criteria. This collaborative work ensures physical and digital structures are integrated seamlessly.

Specifically, USAISEC participates in working groups to author, edit, and publish technical criteria and standards for inside plant (ISP) and outside plant (OSP) infrastructure. ISP infrastructure consists of the telecommunications spaces, pathways, cabling, and components inside a building that support voice, data, video, and smart building systems. OSP infrastructure comprises the physical backbone outside the buildings, including buried copper and fiber optic cables, aerial lines, and telecommunications vaults.

These standards are integrated into the Unified Facilities Criteria (UFC) and Unified Facilities Guide Specifications (UFGS). Because UFC and UFGS govern all armed forces facilities and real property projects across military departments, defense agencies, and field activities, USAISEC's contributions have a department-wide impact.

"Implementation of these guides and specifications has department-wide impacts across the armed forces," said Michael Bitner, director of the USAISEC Engineering Directorate, Fort Detrick, Maryland. "USAISEC's active participation in working groups and contributions to these updates are vital to ensuring modern technologies, methodologies, and installation standards integrate for optimal project outcomes."

Inter-Service Collaboration and Distribution

The UFC program provides planning, design, construction, sustainment, restoration, and modernization criteria for armed forces facilities. This joint program is administered by the U.S. Army Corps of Engineers (USACE), Naval Facilities Engineering Systems Command (NAVFAC), and Air Force Civil Engineer Center (AFCEC). Recognizing the value of USAISEC's telecommunications expertise since the inception of the program, USACE consistently invites the command to help author these critical global standards. USAISEC participates in weekly meetings with USACE and other partner representatives to review telecommunications, power, and HVAC requirements, ensuring the criteria remain state-of-the-art standards.

These standards are distributed exclusively in electronic format through the Whole Building Design Guide (WBDG) website, making these standards available to the public at no cost. The National Institute of Building Sciences manages the WBDG website. Authorized by Congress, the WBDG staff conducts research, establishes performance criteria, and promotes standards that advance transformational technologies in the built environment. Among these standards, UFC 3-580-01 (Department of Defense [DoD], 2024) is particularly critical. This standard details design criteria for telecommunications spaces, pathways, cabling, and interconnecting components necessary to support voice, data, video, smart buildings, and the internet of things.

A formal change request process for criteria allows users to submit feedback. USAISEC reviews these requests, notifies requesters of the outcome, and provides the technical rationale behind approvals or rejections. This global collaboration with military services and industry partners keeps USAISEC's engineers at the cutting edge of technology.

Engineering the Physical Backbone

While the UFC provides design criteria, the UFGS provides the comprehensive construction specifications that military services use for contract execution. These specifications establish mandatory

language for construction contracts, ensuring consistent safety, sustainability, and functionality standards across all Department of War projects.

The Tri-Service Engineering Senior Executive Panel governs the working groups that prepare these standards. For example, UFGS 33 82 00 (DoD, 2020) covers OSP infrastructure, including campus distributors, outside copper and fiber optic cable media, and associated hardware. USAISEC's deep expertise in cabling and wiring provides the technical foundation for the physical backbone of installation IT networks, ensuring buried fiber optic cables and telecommunication vaults remain robust and resistant to physical or cyber compromise.

The Path to Mission Assurance

As military installations become increasingly interconnected, the distinction between physical facilities and digital infrastructure continues to blur. Through relentless engagement in inter-service working groups and technical collaboration, content contributions, and meticulous review of these standards, USAISEC ensures Army installations are engineered to survive and adapt to any operational disruption. By embedding physical and digital resilience into the foundation of the Army's assets, USAISEC acts as a powerful force multiplier, directly contributing to the capability of the Army to fight and win the nation's wars.

As the Army modernizes its footprint, USAISEC stands ready to assist organizations across the enterprise in standardizing communications infrastructure and delivering integrated operational and information technology solutions. To request USAISEC's engineering support, send an email to usaisec@army.mil.

About the Author



Larry Poole is a senior systems engineer and technical advisor at USAISEC. He specializes in physical-to-digital systems integration, cyber-physical security standardizations, and network resiliency across Department of War facilities. Poole represents the Army on several joint-service committees responsible for updating the UFC and UFGS. He has an electrical engineering degree from Old Dominion University. Poole has worked for the Department of War for 40 years and has dedicated 26 of those years working for USAISEC.

References

Department of Defense. (2020). Outside plant (OSP) telecommunication cabling and hardware (UFGS 33 82 00). Whole Building Design Guide. https://www.wbdg.org/ffc/dod/unified-facilities-guide-specifications-ufgs/ufgs-33-82-00

Department of Defense. (2024). Telecommunications interior infrastructure planning and design (UFC 3-580-01). Whole Building Design Guide. https://www.wbdg.org/ffc/dod/unified-facilities-criteria-ufc/ufc-3-580-01

10 U.S.C. § 101 (2021). https://www.law.cornell.edu/uscode/text/10/101



'From the Edge to the Enterprise'

Signal Corps welcomes 44th Chief of Signal

Laura Levering
U.S. Army Signal School

FORT GORDON, Ga. – The U.S. Army Signal Corps welcomed its 44th Chief of Signal and Signal School commandant in a change of responsibility ceremony at Signal Theater, July 31, 2026.

Col. Julia Donley relinquished her duties as the 43rd Chief of Signal and commandant to Col. Bernard Brogan, marking the official end of Donley's 26 years of military service.

Maj. Gen. Ryan Janovic, commanding general of the U.S. Army Cyber Center of Excellence and Fort Gordon, served as presiding officer for the ceremony. Prior to Janovic's remarks, guests were treated to a brief demonstration highlighting the evolution of communication – made possible by the men and women of the Signal Corps.

From semaphore flags to modern-day communication kits and everything in-between, "the history of the Signal Corps is a great one – it is one that you can see in different parts of the installation, and there is a lot to be proud of," said Janovic.

Widely known for her involvement in bringing awareness to the Signal Corps' "Hello Girls," the commanding general described Donley as "one of the most stalwart supporters" of the Signal Regiment's history and traditions. Perhaps just as noteworthy, if not more so, has been Donley's unwavering commitment to the men and women serving in today's Signal Corps – as well as those of the future.

"There is no better officer than you to do what we needed to be done, and you did it in a way that is professionally relaxed – yet were willing to challenge convention – willing to say, 'That is not right,' willing to push boundaries, willing to go faster than we've gone before, and you do it in a way that is

Col. Bernard Brogan, 44th Chief of Signal, receives the Signal Regiment colors from Maj. Gen. Ryan Janovic, commanding general of U.S. Army Cyber Center of Excellence and Fort Gordon, signifying the change of leadership. ***(Photo by Laura Levering, U.S. Army Signal School)***



Staff Sgt. Dylan Pirtle, training developer, U.S. Army Signal School (left), and Lily Romagnoli, of Evans, Georgia, participate in a brief demonstration highlighting the evolution of communication throughout Signal Corps history. ***(Photo by Laura Levering, U.S. Army Signal School)***

uncharacteristically always about protecting our Army's Signal Regiment," Janovic said of Donley.

At a time when the nation is engaged in war, Janovic acknowledged there are service members currently serving in harm's way, which has led to many difficult discussions and critical decision making. Through it all, Donley kept those service members' well-being at the front of her mind.

"Thank you – publicly – for keeping us focused on the quality of what comes out of our classrooms, the readiness that goes into these formations, the commitment to excellence across the Signal Regiment, and then the recognition that they are in hard, hard places doing what our nation asked them to do," Janovic said.

Turning to Brogan, Janovic tried to articulate the weight of responsibility he is being trusted with in leading the force into the future. His advice to the new commandant was two-fold: turn to others for assistance and remain mindful of the people behind the mission.

"You will do great things with the love of this family, with the mentorship that has existed for years, with the mentorship that's going to rise out of the seats of the NCO Corps … and remember your task is to delver to our Army the finest trained young men and women the Signal Regiment has ever known," Janovic said. "Do that and everything else is secondary."

Taking to the stage for her final time and having been awarded the Legion of Merit moments before the official ceremony, Donley's remarks focused on gratitude and the countless people who contributed to her success.

"As awards get fancier and higher up, it's because they're not about individual effort anymore; they are a reflection of all the people the leader worked with, and those peoples' hard work, efforts, and heart to get the mission done, Donley said. "I have been very lucky over the course of my 26 years to be a part of some really wonderful teams, and the Signal School and the Regiment – I am super proud to have been a part of that as the culmination of my career."

Brogan also expressed a plethora of gratitude as he took to the podium for his first remarks as the 44th Chief of Signal, which he described as "a profound opportunity." He then proceeded to share thoughts about how got to that point in his career.

"Number one: Trusting in God and knowing there is no weapon against me that shall prosper," Brogan said. "Number two: Command Sgt. Maj. Craig Johnson … Number three: Be a good teammate … Number four: Nothing replaces hard work."

Brogan elaborated on each point and pledged to lead the Signal Corps with those same principles, while emphasizing that he will ensure that all ranks receive training required to "protect themselves and enable data from the edge to the enterprise – for warfighting and the use of modernized command and control systems – which our nation's warfighters need to deploy, fight and win."

"I thank you today for taking your time to come – far and wide – to see a young man from Alabama take some responsibility to help our nation," Brogan concluded. "I stand ready to fight and defend."

Master Sgt. Stephen Tackett, U.S. Army Signal School, presents a bouquet of flowers to Mrs. Reon Brogan, wife of Col. Bernard Brogan, the 44th Chief of Signal and Signal School commandant. ***(Photo by Spc. Samantha Powers, U.S. Army Cyber Center of Excellence)***

