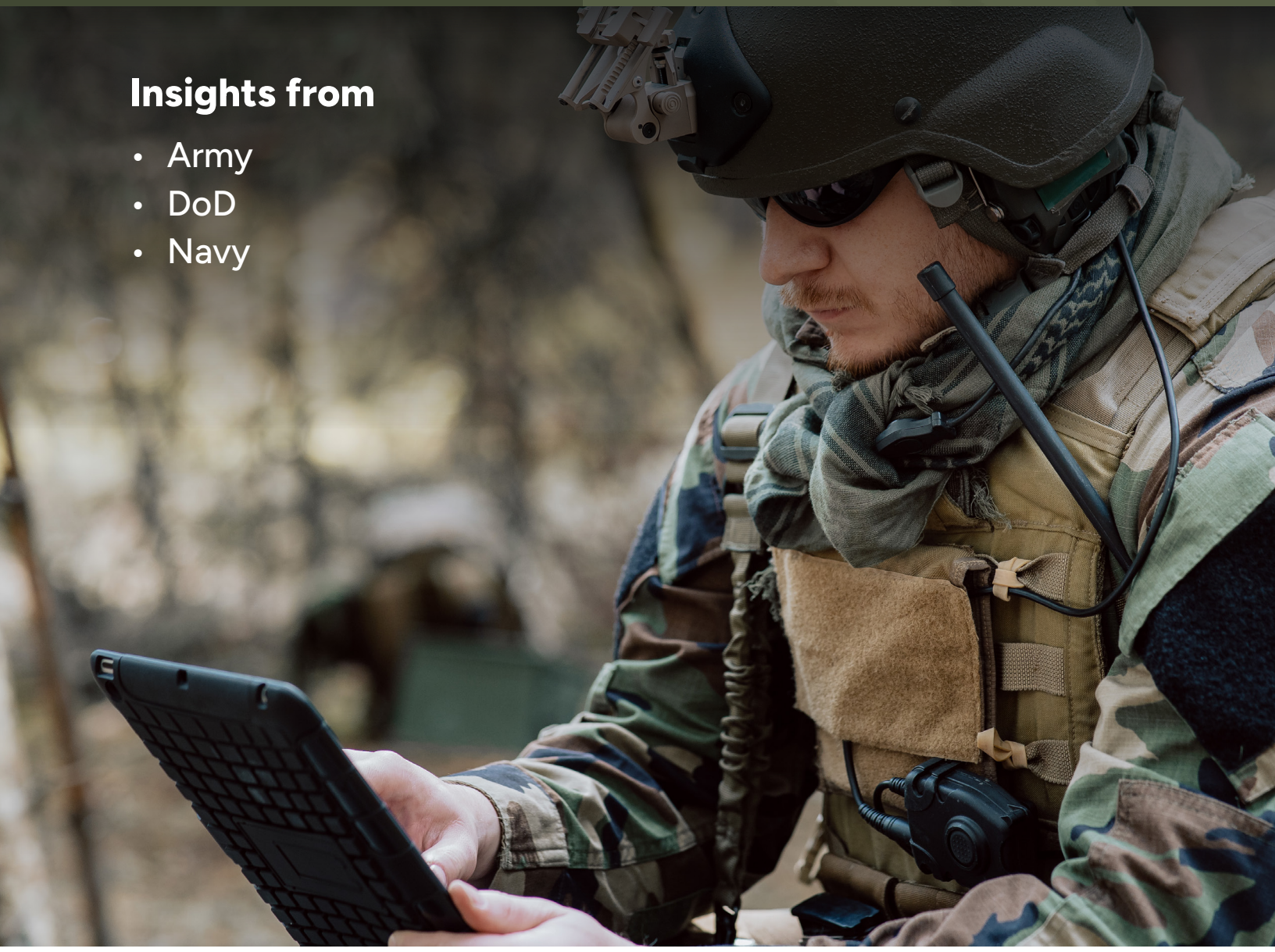
FEDERAL NEWS NETWORK

EXPERT EDITION

DoD vision: Connect anything, provide access anywhere



Insights from

- Army
- DoD
- Navy

BROUGHT TO YOU BY verizon

It's time to upgrade your IT infrastructure.

We know you need the right network system to keep up with the critical communications challenges you face. Let us help with Verizon's Network as a Service. Our managed service offerings provide your military operations with a secure, scalable and virtualized network. Improve mission readiness today, with the network built for tomorrow.

Learn more at verizon.com/defense

verizon

TABLE OF CONTENTS

From the edge and back again

What's clear is that the Defense Department has a gameplan for connectivity. It's straightforward: anything, anywhere, anytime.

Getting there might be less so though and requires taking advantage of networks and capabilities both inside DoD and from industry — commercial 5G blended with military-unique connectivity.

"What would be great is if those networks that we project forward also work with the technology we use on the public networks so that it's very seamless to the user," offers Ken Andrews, principal investigator for 5G efforts at Joint Base Pearl Harbor-Hickam. "We could deploy warfighters, give them SIM cards, give them phones, no matter where they're operating. That, I think, is our vision."

Across the department and the military services, the push is on to achieve that vision. This e-book takes a detailed look both at these efforts at the macro and micro levels — sharing challenges, successes and insights on efforts to connect anything and provide access anywhere.

Rethinking the way teams approach the idea of connectivity has had to change fundamentally, points out Col. Mike Kaloostian, director of transportation and network security for Army Futures Command.

"We need to think tactical first and then operational and strategic," he said. "If we're not defining tactical edge at the platoon, we are getting it wrong."

In pages ahead, you will learn how DoD organizations are aiming to get it right — from the edge and back.

Vanessa Roberts
Editor, Custom Content
Federal News Network

Pentagon rolls out strategy for private 5G

BY JARED SERBU

The Defense Department has a new plan to deploy its own 5G wireless systems on military bases and other operating locations around the world, hoping to fill in the gaps not served by commercial telecommunications companies in, for example, remote and austere locations.

The new private 5G deployment strategy — signed by acting DoD Chief Information Officer Leslie Beavers in October 2024 — calls for "accelerated" deployments of DoD-only 5G networks but with a tailored approach that takes each location's needs into consideration.

Notably, the strategy makes clear that the department's preferred choice, in most cases, is to make use of the trillions of dollars in 5G infrastructure that commercial firms have already deployed around the world. But the military services will also need options to create their own networks where there simply are no commercial towers.

"A key aspect to DoD's IT modernization effort is to leverage 5G networks, both commercial and private, to deliver ubiquitous high-speed connectivity for mobile capabilities," Beavers wrote in a letter accompanying the strategy. "Commercial networks offer core 5G services to a broad range of users across densely populated portions of military installations. … However, DoD acknowledges that under certain circumstances, commercial networks may not fulfill an installation's requirements. Private networks can augment or supplement commercial services, as they are tailored to the specific

A key aspect to DoD's IT modernization effort is to leverage 5G networks, both commercial and private, to deliver ubiquitous high-speed connectivity for mobile capabilities.

Leslie Beavers
Acting Chief Information Officer, DoD

installation's mission needs, security and military-unique capabilities."

Private 5G needs already apparent in INDOPACOM

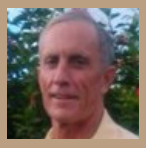
Since the release of DoD's broader 5G strategy in 2020, the military services' experimentation with the latest generation of wireless technology has borne out the need for private 5G, in, for example, further-flung areas of the department's Indo-Pacific Command.

Kurt Andrews, principal investigator for 5G efforts at Joint Base Pearl Harbor-Hickam in Hawaii, said the commercial networks DoD has been using in early efforts offer 99.999%, or five nines, uptime. Technologists have successfully used those wireless links to, for example, connect quadcopters that help technicians with on-base aircraft maintenance.

"But there's obviously going to be places as we look west — islands that we call places, not bases — where maybe there won't be networks," Andrews said at a Honolulu conference organized by AFCEA in fall of 2024. "We all want to be prepared for that, and we're looking at the ability to project forward, to bring 5G into that world. What would be great is if those networks that we project forward also work with the technology we use on the public networks so that it's very seamless to the user. We could deploy warfighters, give them SIM cards, give them phones, no matter where they're operating. That, I think, is our vision.

Defense officials said more detailed guidance on exactly how the military services should implement private 5G will likely be coming in 2025.

> But there's obviously going to be places as we look west — islands that we call places, not bases — where maybe there won't be networks. "We all want to be prepared for that, and we're looking at the ability to project forward, to bring 5G into that world.



Kurt Andrews, Principal Investigator for 5G Efforts, Joint Base Pearl Harbor-Hickam

But the strategy also hints that DoD may be leaning toward an enterprise approach to private 5G services. Exactly what that might look like is still unclear: According to the document, the department is still conducting an analysis of alternatives to decide whether DoD should develop its own "core" worldwide 5G network, or whether the military departments should buy their private implementation "as a service" from commercial providers.

The strategy's release comes roughly one year after Congress made its own push

to get the military to adopt private 5G. As part of the 2024 Defense authorization bill, lawmakers ordered the department to draw up a strategy that, among other things, streamlines the process for commercial wireless companies to build wireless infrastructure on bases and implements a modular approach that lets new technology be inserted and upgraded over time.

Open 5G standards

To answer the "modular" part of the equation, the final strategy leans on the existing Open Radio Access Network (O-RAN) concept, which emphasizes interoperable radio standards, hardware-agnostic networks and the incorporation of cloud technologies. Officials said they would encourage the development of an O-RAN "ecosystem" by prioritizing those approaches in the department's acquisition decisions, and by conducting more prototype work on how to adopt open source O-RAN specifications like the RAN Intelligent Controller (RIC).

And Defense officials have significant reasons to want communications networks that operate with secure, well-understood interfaces — whether commercial or private — particularly in areas such as logistics and for increasingly advanced systems that rely on AI algorithms that require frequent software updates.
"In a sustainment realm, you could imagine hundreds or thousands of unmanned systems, which need to be ready to be deployed within a fairly constrained timeline — but that deployment may be one year out or three years out, we don't know," said Chris Murphy, science and technology advisor to the Navy's Pacific Fleet.

"If I've got them stacked in a warehouse, how do I support over-the-air updates to ensure that the continually developed software stacks are routinely deployed to these systems? It gets to the ability to leverage in-place infrastructure without having to deploy wired or more bespoke systems. That also gives you a lot of flexibility to move where these things are stored, from maybe a desert to a coastal city. You can take advantage of a lot of the local infrastructure to support that sustainment … 5G, and specifically leveraging commercial and public infrastructure to support that, is huge."

> You could imagine hundreds or thousands of unmanned systems, which need to be ready to be deployed within a fairly constrained timeline. … It gets to the ability to leverage in-place infrastructure without having to deploy wired or more bespoke systems.
>
> ***— Chris Murphy, Science and Technology Advisor, Navy Pacific Fleet***

Army makes IT organization changes in pursuit of unified network

BY JARED SERBU

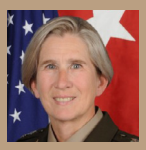
The Army began fiscal 2025 with some notable changes to the organizations that have long had a hand in building and maintaining its network and communications capabilities, all with the hope of finally achieving an objective officials have talked about for a decade or more: an IT and data ecosystem that gives soldiers the same capabilities irrespective of where in the world they happen to be.

The changes weave together themes the Army has discussed extensively in recent years: the concept of a unified network rather than separate enterprise and tactical networks, and that also makes data ubiquitous and secure. But officials acknowledge that they're also reflective of a culture change that will finally enable all of those things to happen.

For one, the Army's Network Enterprise Technology Command (NETCOM), is pivoting from being the organization that focuses mainly on operating and maintaining its network infrastructure to more of an all-in-one provider for critical services like cybersecurity and identity management.

"We're going to really start focusing on not only delivering that network, but everything that's going through that network. … We're going to have global collaboration tools that are going to be available to us, both horizontally and vertically — letting our theaters talk to one another, and going up and down through the Army," Maj. Gen. Denise McPhail, NETCOM's commander, told attendees at a recent AUSA conference. "It really means being able to pick up your system [when you deploy] and not have to re-image

> We're going to really start focusing on not only delivering that network, but everything that's going through that network.



Maj. Gen. Denise McPhail, Commander, NETCOM

it over and over. Now, you're not going to have to do that. You're going to have seamless movement across the globe."

Organizational rebranding

The Army has also made some organizational nomenclature changes over the last several months that are in some ways cosmetic, but that officials say reflect a genuine cultural shift: a recognition that the Army's networks, its data and its connectivity are inextricably linked.

That's a reality the service may not have fully realized as recently as 2018, when one of the largest reorganizations in its recent history resulted in the standup of Army Futures Command and the creation of what has, since then, been called the Army Network Cross-Functional Team.

That CFT is now called the Command and Control Cross-Functional Team, said Maj. Gen. Patrick Ellis, who took lead of the team in early 2024.

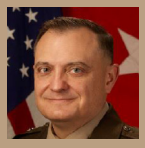
"That really reemphasizes the importance of the fact that we're taking on command and control — we're so much more than just a network. The network needs to be something that leads to data, and data leads to better decisions," he said. "Part of the reason we've been redesignated is to reflect where we've been. But my job is also to put the commander back in command and control and to enable the commander to make better, faster and more optimized decisions at a high rate of speed."

One acquisition organization for unified networkfor

One way to do that is to make the Army's acquisition decisions around its networking capabilities much more flexible — especially the ones that relate to the exact types of equipment soldiers might travel with and deploy as part of command posts in distant locations.

That's largely the job of another organization that has a new name: the Program Executive Office for Command, Control, Communications and Networks (PEO-C3N). Until recently, it was called PEO-C3T — with the T standing for tactical.

> We want to put tools in the hands of the commanders that allow them to scale up and scale down, reconfigure their command post as they need to — based on the mission and how the commander chooses to command.



Maj. Gen. Patrick Ellis, Leader, Command and Control Cross-Functional Team, Army

But the Army has decided it makes much more sense to have one acquisition organization in charge of network-related procurement decisions, said Mark Kitz, program executive officer for the newly named organization.

"You're seeing requirements and acquisition integration across our entire unified network. PEO-C3N now owns the entire unified network, but you're seeing collaboration between the Command and Control Cross-Functional Team, NETCOM and the G6 community," he said. "We are now truly treating this network as a unified network, and I would say that behavior in industry has to match this cultural behavior on the government side."

As for what that means on the ground, the Army said it wants vendors to offer solutions that are compatible with ubiquitous connectivity and the idea that there's never going to be a one-size-fits-all approach to an Army command post in the future.

> We are now truly treating this network as a unified network, and I would say that behavior in industry has to match sort of this cultural behavior on the government side.

Mark Kitz, Program Executive Officer for Command, Control, Communications and Networks

Instead, commanders will need the flexibility to tailor their approaches to the connectivity options available to them and the mission requirements in front of them.

"A lot of that looks like things that you're already familiar with — low Earth orbit capability and some additional radio capability," Ellis said. "We're enabling the command post by making it a little bit more modular, as opposed to having a big, monolithic command post where everyone looks the same. We want to put tools in the hands of the commanders that allow them to scale up and scale down, reconfigure their command post as they need to — based on the mission and how the commander chooses to command. That's something we were able to observe watching the conflict in Europe: the command posts were constantly changing as a result of the battlefield."

Next Generation Command and Control

The Army is hoping to tie all those efforts together — and figure out where to go next — via an initiative called Next Generation Command and Control.

The service published a request for information in September 2024 asking vendors for input on how the Army might build a system-of-systems approach to ways that would let companies plug in to the Army's Unified Data Reference Architecture — the service's new framework for making data more accessible across the entire organization.

"We're going to look hard at data integration across all domains," said Maj. Gen. Jeth Rey, deputy chief of staff, G-6. "We're going to look at more AI and machine learning that we're going to put against that data in order to enrich it for the user and for the warfighter.

> We're going to leverage cloud at the edge computing because we want to bridge our tactical and strategic as we look at the unified network.
>
> 
>
> *Maj. Gen. Jeth Rey, Deputy Chief of Staff, G-6, Army*

We're going to strengthen data in our governance, in our security across domains as well. We're going to leverage cloud at the edge computing because we want to bridge our tactical and strategic as we look at the unified network."

DoD sees strong potential in opening up new spectrum

BY JASON MILLER

The future design of the Army's network must start at the edge and work backward. Long gone are the days where any military service builds a network that starts at a post, camp or station and then extends to the tactical edge.

"For too long we have thought about the network from a strategic, operational and *then* tactical perspective. We can't think that way anymore," said Col. Mike Kaloostian, director of transportation and network security for Army Futures Command, at the Army Technical Exchange Meeting 13. "We need to think tactical first and then operational and strategic. If we're not defining tactical edge at the platoon, we are getting it wrong."

This realization for the Army — and really every part of the Defense Department — comes because the only thing that matters for service members is having access to data to drive real-time and critical decisions.

"We can't go back to the cloud for everything we do. It may not be available. So what we need is to be able to process data at the tactical edge," Kaloostian said. "What new edge computing capabilities exist that we can experiment and learn about now? How can we deploy microservices to the edge so we don't have to go back to the cloud for everything?"

Proving ground for DoD user cases

One way DoD is addressing the challenges around bandwidth, application latency and connectivity at the edge is by seeking to open up the Lower 37 GHz band (37-37.6 GHz) to federal and nonfederal organizations.

DoD and the National Telecommunications and Information Administration (NTIA) recently completed a study that recommends creating a co-sharing framework with the Pentagon getting access to a certain section of the band that could create a proving ground for technological solutions for unique military user needs.

The report is the first deliverable under the National Spectrum Strategy created by the White House in November 2023. It directed DoD and NTIA to examine a key set of bands to ensure U.S. leadership in spectrum-based services now and into the future. The strategy identified the Lower 37 GHz band as one of five spectrum ranges where an in-depth study is needed

to determine ways to repurpose it to drive innovation.

In a request for comment in August 2024, the Federal Communications Commission said the current record on potential uses of the 37-GHz band is limited. But public and private sector experts "foresee uses including fixed wireless broadband, point-to-point links, Internet of Things networks, device-to-device operations, augmented reality applications, smart cities, smart grids as part of private networks."

In the DoD-NTIA report, experts also said the band is "well-suited to deliver high-speed, low-latency multigigabit and 5G services over short and medium distances."

> For too long we have thought about the network from a strategic, operational and then tactical perspective. We can't think that way anymore.
>
>
>
> ***Col. Mike Kaloostian, Director, Transportation and Network Security, Army Futures Command***

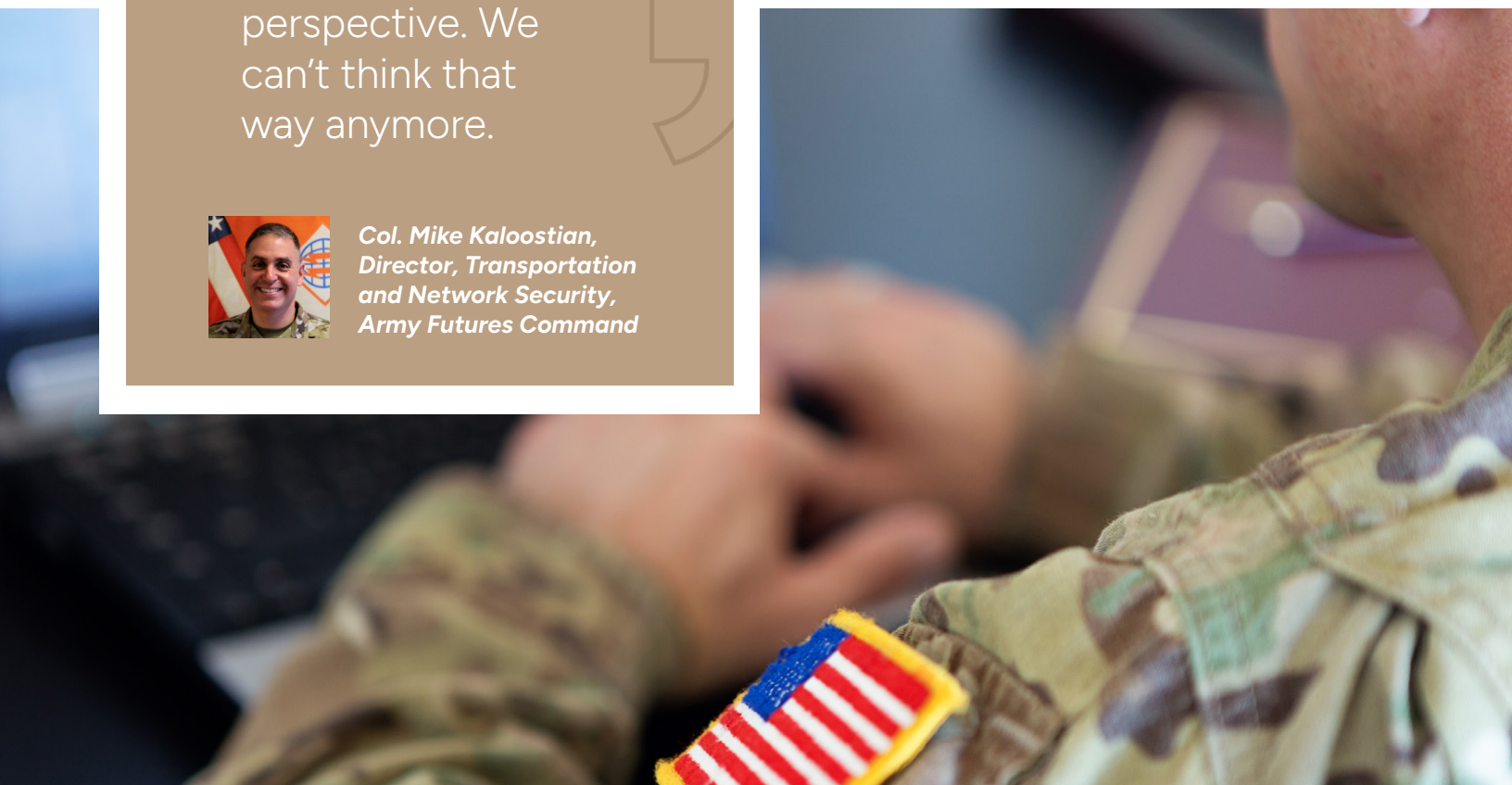
The report also noted "the band's ability to support concentrated deployments over small geographic areas advances sharing."

More research needed

It's those potential uses for the band that are attractive to the Pentagon. In the DoD-NTIA study, the military laid out two potential areas where it wants to pursue further research:

The first is around unmanned systems. "This spectrum can provide unmanned systems with high-bandwidth data for force protection video, communication, lifesaving medical supplies, logistics, sensor power restoration, and undersea and maritime capabilities," the report said.

The second area is around wireless power transfer. Within that area, DoD would like to research whether the spectrum could deliver untethered power to and through unmanned systems,



wireless communication systems, underwater vehicles, sensor recharging, satellite to aircraft, space to moon and several other areas.

"DoD is interested in collaboration with industry on wireless power transfer equipment development, which would operate within the confines of the military priority band," the report noted. "Wireless power transfer to vehicles has the potential to benefit DoD in many ways as this technology resolves battery drainage challenges for mobile vehicle radios, provides tighter beamwidths, is more cost effective and may offer better safety standards than the current power transfer at higher frequency bands."

Reducing the power need for systems and applications is a major focus for the Army.

> We have to consider over time how to improve our capabilities, especially getting data to the edge. We are working toward finding an edge computing solution where we can transmit data more quickly.
>
> ***— Army Futures Command's Col. Mike Kaloostian***

C2 big 3 focuses

The Amry has identified three chief focus areas for its command and control fix program.

Lt. Col. Jon Nielsen, 1-502nd battalion commander in the 101st Airborne Division, detailed them during the Army Technical Exchange Meeting 13:

- **Research power management:** There is a big power requirement for all hardware capabilities, Nielsen said. A power recharge capability going from a 24-hour window to between 72 and 96 hours would make a huge difference, he said.
- **Reduce weight:** Managing the individual hardware is difficult because each type adds weight, and packing room is limited, he said. Reducing power and weight is a requirement for any new C2 solution, Nielsen said.
- **Build interoperability into all systems:** Ensuring all systems and applications are interoperable remains a long-term goal, he said.

"We now have data at the edge. We can communicate faster and more accurately, and it's a significant improvement for our team and our lethality," Nielsen said. "But we have to consider over time how to improve our capabilities, especially getting data to the edge. We are working toward finding an edge computing solution where we can transmit data more quickly."

Lincoln returns to port after proving out 'game changing' connectivity

BY JARED SERBU

The USS Abraham Lincoln returned to its homeport in San Diego in December after a multimonth tour at sea — including an unusually long stint of 107 days without a port call. But the Nimitz-class aircraft carrier had something that's been unheard of until now: high-speed internet connectivity, even when it was thousands of miles from shore.

The connectivity sailors had available during the Lincoln's sea tour was the biggest demonstration to date of a Navy project called Sailor Edge Afloat and Ashore, which aims to bring shore-grade communications to underway ships, and the related Flank Speed Edge, the Navy initiative to extend its cloud computing offerings to places where bandwidth is a major challenge.

Using proliferated low Earth orbit satellites and 5G cellular networks, the Lincoln was able to transmit and receive volumes of data that previously would have been unthinkable in an afloat environment: about 8 terabytes per day.

But the project first started more than two years ago, when officials realized the technology was now available to connect ships to networks for purposes other than mission critical tactical and business applications.

"In August of 2022, we went full in on trying to figure out that solution. We also wanted to provide connectivity in a meaningful way for sailors because we're all connected in the world," Capt. Kevin White, the Lincoln's combat systems officer, told Federal News Network in an at-sea interview this month, shortly before the ship's return home. "When you disrupt connections by going to sea, you disrupt one's own identity and how they conduct their life. We believe that as you enable connections, it's a way to enable retention in the United States Navy. It's also a way for people to feel a more meaningful connection to their job."

Layered approach to personal, mission-related connectivity

During the five-month deployment — covering some 78,000 miles — the crew used the new connectivity for everything from YouTube and Instagram to Navy business applications and the warfighting systems that the military's older, much

slower satellite communications links were first set up to serve decades ago.

And while the new Sailor Edge connections offer orders of magnitude more bandwidth than traditional military SATCOM links, planners also had to keep in mind that they were going to be serving a crew of 6,000 people aboard the Lincoln. That meant some amount of rationing needed to be taken into consideration.

Still, as long as the ship was operating in areas where network connectivity wasn't an issue for operational security, there generally turned out to be plenty of bandwidth to go around, White said.

"What we did was we took a layered concept. One thing we expect is for sailors to be able to text message or call home anytime, so we built a series of layers in how we bucket the traffic and then how it is prioritized amongst available bandwidth," he said. "We prioritize our business applications. We have quality of work, traffic-shaping layers, and those are our highest priority. But it also turns out that those are really kind of low-traffic sources. And then we have many quality of life traffic shaping layers … at any given time. The layers are provisioning bandwidth across those services."

> When you disrupt connections by going to sea, you disrupt one's own identity and how they conduct their life. We believe that as you enable connections, it's a way to enable retention in the United States Navy."
>
> ***— Capt. Kevin White, Combat Systems Officer, USS Abraham Lincoln***

Each sailor on board was given an account to log in to the ship's Wi-Fi network — similar to the portals one might use at a hotel.

"And as they do, that tracks how much data they use, and then we have some mechanisms that enforce where they are allowed to go versus where they are not allowed to go per Defense Department policy," White said. "We actually layer up content based on the value that content provides somebody combined with how bandwidth-heavy it is. I expect everybody to be able to make a phone call and send a text message, and then some level of personal entertainment value. However, it is definitely not unlimited."

Testing the waters with more providers

During long transits far from shore (the Lincoln's tour spanned from the Western Pacific to an unexpected deployment to the Middle East), the high-speed links were supplied mainly by Starshield, SpaceX's P-LEO offering for government customers. But White said several other satellite

providers have expressed interest in the Sailor Edge effort.

"We've had some awesome opportunities to exercise some of those game-changing capabilities," he said. "It's kind of like if you build it, they will come, and we've now seen a full force effort of folks interested to scale out both our capability on ships as well as in various shore sites around the world. So that's fantastic, and that was exactly what we envisioned from the start."

But closer to land, the Lincoln's latest deployment also demonstrated the ability to connect the ship to commercial 5G towers at what turned out to be surprisingly long distances.

"We tested a multi-5G cellular aggregation capability with cellular antennas, and the intent of the test was if a ship is in a foreign port, what value does that provide that ship from a cost and a scalability perspective? But we also wanted to see if we could actually get some measurable traffic to pass while we're at sea," White said. "And it worked. It worked phenomenally. I was quite surprised at how far away we were able to pass traffic at sea — in excess of 100 miles. And it just shows the scalability of the Sailor Edge Afloat and Ashore capability as well as how we can integrate with other options and continue to move the needle."

> I was quite surprised at how far away we were able to pass traffic at sea — in excess of 100 miles.
>
> ***— Navy's Capt. Kevin White***

DoD edges toward goal of ubiquitos

BY JARED SERBU

Bit by bit, the U.S. military has been undergoing something of a communications revolution over the last several years: from an aircraft carrier suddenly having hundreds of megabits of bandwidth available on board to the Army moving toward a single network for both its enterprise and tactical communications and communicators in Indo-Pacific Command finding new ways to interoperate with new partners.

It's largely due to recent changes — some policy-related, but certainly some cultural — that have pushed the armed services to embrace the same commercial technologies that have already made ubiquitous connectivity commonplace in most of our lives.

On board the USS Abraham Lincoln, for example, it's largely 5G technology and commercial satellite services that have started to deliver previously unheard of connectivity possibilities to sailors at sea.

But it's not just about connecting people. The sought-after ubiquitous connectivity also brings new opportunities to connect data-producing devices in new and innovative ways.

"It could be anything, perhaps a sensor, a drone, a human. It could be wired of wireless," said Ken Gonzalez, director of federal solutions architecture at Verizon. "It's not limited to what you are connecting to. You need to access data that's remote. You need to access information that is perhaps with the person who is 100 feet away from you. The reality is that we are no longer bound by the communications constructs of the past five to seven years."

> The reality is that we are no longer bound by the communications constructs of the past five to seven years.
>
> 
>
> ***Ken Gonzalez, Director of Federal Solutions Architecture, Verizon***

New demand for upstream network flows

This new communications paradigm also has major implications for how networks are designed and what they need to be able to do. Both in the private sector and

in the military, an everything-connected world doesn't just increase the demand for bandwidth — it often means each network-connected node must be able to transmit as much data as it consumes.

Historically, that hasn't been the case. Many end users have tended to be connected to networks with fairly large downstream data pipes and narrow upstream ones.

"We now use concepts like edge computing because some applications require that compute power be as close as possible to the user," Gonzalez said. "But that is not always feasible, which means now you need to be in a position to understand that you need to have a network that can support massive amounts of data being transferred up to be processed and on the way down, as the result of a computation that will allow you to have the information that you need."

The increasing use of artificial intelligence to parse and analyze data to aid in real-time decision-making also has changed connectivity demands, he said.

"You now need to upload as much data, or perhaps more data, than you're downloading," Gonzalez pointed out. That requires being smart both about the kind of data that an organization transfers and when.

"If you're in a mission critical environment where the data needs to be extremely low latency, you need to be able to classify it as such and separate critical data flows from those that are not mission critical," he said. "You need to be smart about how to leverage your network and perhaps suppress some types of data that don't need to be transferred at a specific time — or data transfers that could be done at off-peak times."

A move to transport-agnostic networks

A concept that's risen to prominence within DoD in recent years is transport-agnostic communications. Military leaders want to give commanders the flexibility to use whatever data pathways happen to be available to them, wherever they happen to be operating around the world.

As Maj. Gen. Jeth Rey, deputy chief of staff, G6, shared at a recent Army Technical Exchange Meeting: "We have tried to find a way to get to data-centric using agnostic transport to move the data as freely as possible to where it needs to go, a cloud-enabled asset to catch and move the data, and then, obviously, you need a layered security architecture. We want a multilevel security architecture where we can move the data from one classification to another seamlessly."

This is a big change. DoD is largely accustomed to communicating over networks it controls. Now, the challenge is doing it securely over physical networks it doesn't control — and in some cases, overseas for example, perhaps networks it doesn't particularly trust.

But those challenges can be solved by applying zero trust principles and approaches like software-defined networking that abstract the network from the copper, fiber or airwaves DoD uses to move data around.

The key, Gonzalez said, is ensuring security is considered at the same time that these networks — even virtual ones — are being designed, not as an afterthought or a bolt-on.

"When we were used to point-to-point connectivity, there was a really good way to know what was connected to what. But as we're going into a world in which you now have hybrid networks, you have elements that are connected through the internet. You have others that are connected through an overlay. And you still have other things that are connected point to point," he said.

But hybrid network environments need a way to "homogenize" the connectivity, which can come in the form of overlays, Gonzalez said.

These overlays will "provide not only the connectivity but the segmentations over the multiple networks underneath," he explained. "So when it comes to security, let's make sure that folks are not separating the network and the connectivity when it comes to design, and the way they're thinking about servicing the users."

A shift in network procurement requirements

What's more, Gonzalez said, security offers an area in which DoD and other federal agencies can improve their odds of success by designing procurements that are more outcome-based and less focused on predefined technical requirements.

Operating in a more outcome- or mission-driven way gives vendors much more latitude to propose solutions that might not arise during a more traditional and rigid requirements process, he said.

"Whenever we have the opportunity to understand the objectives, we are

positioned to provide different thought leadership and bring forward ideas that today the mission owners may not be aware as possible. When you start with objectives first and then you define your requirements, everybody wins," Gonzalez said.

"A lot of the limitations that we have as an industry are defined by the government. Every single one of these solicitations needs to be fair for everybody … but if the process — at the request for information or sources-sought stage — allows us to be a little bit more creative and provide solutions, we will be really leveraging the infrastructure and technical expertise that we have gained across an entire book of business and provide a better solution to meet the objectives of the mission."

> When it comes to security, let's make sure that folks are not separating the network and the connectivity when it comes to design, and the way they're thinking about servicing the users.
>
> ***— Verizon's Ken Gonzalez***

Watch the full discussion between Federal News Network's Jared Serbu and Verizon's Ken Gonzalez on modernizing Defense networks