

SPECIAL BULLETIN REVIEW

Future of Edge Computing at DoD

Insights from

- Air Force
- Army
- DISA
- Navy

BROUGHT TO YOU BY

verizon

We build smarter future-ready bases, so you can focus on the mission.

Verizon's intelligent edge network unifies IT systems and IoT devices to drive our smart base solutions. They can help create more realistic training exercises and inform faster data-driven decisions, so your team is better equipped for the mission ahead.

Learn more at [verizon.com/smartbase](https://www.verizon.com/smartbase)



verizon^v

TABLE OF CONTENTS

DISA sets plan for zero trust evolution	4
Army continues push toward tactical OCONUS cloud	6
Navy's edge strategy views hardware as disposable	8
Air Force builds on ABMS test successes	11
Army embraces consolidated network with UNO	13
Purposeful innovation offers path to modern networks	17



'At the edge' aptly describes DoD's world

Perhaps more than other agencies, the Defense Department truly understands what it means to make decisions "at the edge" – whether that's a command deployed to a far-off battlefield or staff working at far-flung permanent but remote DoD locations (Eielson Air Force Base in North Pole, Alaska, for instance).

In fact, between its enlisted and civilian staff, DoD is home to nearly 3 million federal employees – a mix of active-duty and reserve service members and civilian personnel – working at locations permanent and temporary around the globe.

The department therefore has long focused on how to get actionable information to the users who need it in a timely and secure manner. Given the complexity and size of the department, that's not been easy.

Now, with a cloud-first, software-defined everything approach, DoD and the military services are intent on achieving network dominance at the enterprise and tactical edge and helping ensure warfighters can access the data they need when they need it.

"What we need in the future is agnostic hardware whose function is defined by a piece of code," Keegan Mills, acting director of the Marine Corps' Task Force Aquila. "The vision is the code could be written on the fly – and in a very sci-fi world that looks like artificial intelligence – you'd have a network that is constructed for a very specific purpose that may only exist for a very short period of time."

In this ebook, we talk with teams across the breadth of DoD that are working toward the goal of making edge computing not only safe but fast and manageable. It offers a snapshot of the types of efforts taking place departmentwide to help DoD modernize its network operations, and we hope it helps your organization envision what's possible.

Vanessa Roberts
Editor, Custom Content
Federal News Network

DISA already preparing for what's to come after Thunderdome to evolve zero trust



BY SCOTT MAUCIONE

Even though the Defense Information System Agency's main zero trust program is still in its infancy, the organization says it's already looking ahead to see what it can do to improve cybersecurity with its application.

DISA awarded a \$7 million prototype contract for Thunderdome early this year. The purpose of the project is to start building the foundation of its zero trust strategy, a completely new way the Defense Department wants to look at cybersecurity and network architecture.

"Thunderdome reflects a substantial shift to a next generation cybersecurity and network architecture for DoD," according to Chris Barnhurst, DISA's deputy director. "Rooted in identity and enhanced security controls, Thunderdome fundamentally changes our classic network-centric, defense-in-depth security model to one centered on the protection of data and will ultimately provide the department with a more secure operating environment through the adoption of zero trust principles."

Planning ahead for cyber evolution

DISA is considering what is next for Thunderdome as it continues the prototype process, DISA Chief Technology Officer Steve Wallace said at the recent AFCEA TechNet Cyber event.

"We can't jump to the next thing right away, but we knew at the onset that things like data tagging and decisions made based on that tagging were not part of the original Thunderdome," he said. The agency must begin now to develop plans for what's to come next, Wallace said.

To that end, DISA leaders are meeting regularly to ensure the most optimal way forward for cybersecurity and identity management.

"We are trying to pilot a set of capabilities that we've identified as promising," said Brian Hermann, director of DISA's Cybersecurity and Analytics Directorate. "We're partnering with the Air Force as well. We

"Rooted in identity and enhanced security controls, Thunderdome fundamentally changes our classic network-centric, defense-in-depth security model to one centered on the protection of data."

— Chris Barnhurst, Deputy Director, Defense Information Systems Agency

want to evaluate both the performance of those capabilities, as well as the interoperability. Given the size and complexity of our territory, we're not going to have a single vendor or even a small number of vendors be part of this."

DISA laser-focused on SD-WAN and SASE

Thunderdome specifically focuses on software-defined wide area networking (SD-WAN) and secure access service edge (SASE).

Hermann said SD-WAN is providing new opportunities to manage transport infrastructure. With SASE, DISA will be able to help drive edge security by weaving network security and network services into a cloud capability.

"We merge that together with our cybersecurity infrastructure and then we're getting away from a separate set of things for cybersecurity versus transport. It starts to blend together," he said.

"In the Department of Defense, we have a design backbone. We have connections to the separate networks that are part of the services' networks," Hermann explained. "How we manage that transition from their networks to the design backbone will determine whether or not we get the performance that we're trying to achieve with SD-WAN across the network."

The larger goal is to build interoperability within the zero trust model so that DISA can accept variances or different solutions when using it, Hermann said.


Tapping OTAs to award prototype initiatives

DISA used its other transaction authority (OTA) to award the Thunderdome prototype. That method is usually used to set agreements with nontraditional defense contractors. But Hermann said DISA used its OTA power differently in this instance.

"In the Department of Defense, we have a design backbone. We have connections to the separate networks that are part of the services' networks. How we manage that transition from their networks to the design backbone will determine whether or not we get the performance that we're trying to achieve with SD-WAN across the network."

— Brian Hermann, Cybersecurity and Analytics Director, DISA

"The more I thought about it, the more I realized that the reason for using an OTA is because we needed the novel technologies that come directly from the vendors that provide those capabilities, but we needed a knowledgeable layer of vendor integration," he said. "The integration brought those together so that we could ensure that we are addressing the complexity and the size of the DoD networks."

DISA's push for Thunderdome stems from a governmentwide interest in zero trust. Last May, the Biden administration put out an [executive order](#) on improving cybersecurity mandating government agencies stand up zero trust architectures by August 2024. 

'Grand success' of OCONUS edge computing test gives Army momentum to tackle tactical cloud next



BY DAISY THORNTON

The Army is getting closer to fulfilling its ambitions to deliver cloud services to the tactical edge following a pilot test delivering edge computing to Guam, which Army Chief Information Officer Raj Iyer described as a "grand success."

The February test lays the groundwork for the Army's program to establish cloud at commands outside the continental United States (OCONUS).

"The First Corps, based out of Joint Base Lewis-McChord, made it part of one of their experiments to show how they can take mission command on the move using edge computing devices and then to be able to link back to data that was in the enterprise cloud," Iyer told *Federal News Network*.

"And it showed that [this capability] was not only much more resilient than the existing solutions that they had, but the performance, the reliability and the latency [were] far superior than anything that they've been used to. So technically, we know it can work."

The First Corps was able to perform mission command functions from a C-17 Globemaster III over the Pacific Ocean en route to Guam and then later from a naval ship.

The idea is to distribute command and control functions over a series of nodes, rather than centralized in one place, to remain mobile and present less of a target to adversaries.

Building on success of OCONUS cloud edge computing test

Now, Iyer said, the Army is looking at how to cement the test use case as part of its institutional processes and operations.

Over the next 18 months, the Indo-Pacific Command (USINDOPACOM) will run roughly 40 exercises to test this functionality, discover best practices and resolve potential weaknesses.

After laying a foundation with OCONUS, the next step will be to take mission command and warfighting

"It showed that [this capability] was not only much more resilient than the existing solutions that they had, but the performance, the reliability and the latency [were] far superior."

— Raj Iyer, Chief Information Officer, Army

functions to the tactical edge and make them cloud native, as part of Army's ongoing modernization efforts, Iyer said. Because there's a fundamental difference between OCONUS cloud and tactical cloud, he said.

"An OCONUS cloud is essentially running a commercial cloud, say, at an Army base in Germany or Camp Humphreys in Korea," Iyer said.

"These essentially would be Army installations. And then we just work with a commercial cloud service provider like Google, Microsoft or Amazon, and then have them come in and essentially establish compute and storage, and then run it as a service for us."

That has the advantage that those services are operating on sovereign land, and the Army has to work around data sovereignty rules, he explained.

"Having these OCONUS cloud locations on Army posts will ensure that we are staying compliant with those requirements to have control over our data," he said.

Those requirements call for a different operating model. The Army provides the physical infrastructure like floor space, cooling and electricity, and the cloud service providers supply the technical infrastructure, provision it and run it.

The service is currently working with the Defense Department to establish this in both Germany and Korea as a joint asset because these will be the first programs of their kind in DoD, Iyer said.

Army sets sights on tactical cloud needs

A tactical DoD cloud, on the other hand, must be capable of operating in more austere environments.


It could involve satellite communications, for instance. Or, it could also require supporting a unit on the move. Therefore, developing tactical cloud capabilities must involve the additional elements of

"Having these OCONUS cloud locations on Army posts will ensure that we are staying compliant with those requirements to have control over our data."

— Army CIO Raj Iyer

SATCOM connectivity and transport as well, Iyer said. That's what the pilot program with USINDOPACOM and First Corps is focused on.

What's more, this work requires collaboration across DoD, including from the Defense Information Systems Agency and the other military branches because tactical cloud edge computing will typically support combatant commands, he said.

"We meet and chat about this regularly to make sure that we're not duplicating efforts," Iyer said. "Because the brain trust for something as complex as this is just not that much out there. And so we want to make sure that we're leveraging all of the expertise that we each have in our departments." 

How will the Navy ensure network service to the tactical edge? By prioritizing software, treating hardware as disposable



BY JARED SERBU

As part of a decade-long reform effort that the Marine Corps launched two years ago, the service is trying to make itself lighter, more adaptable and more expeditionary. And it'll need an IT infrastructure in line with that broader vision, called Force Design 2030.

If the Marines are going to pull it off, the current thinking is the service will move in fairly short order to a new way of designing and implementing network technology – one which allows the hardware to become an interchangeable, expendable commodity, while all the real work is done in software.

Much of that work falls to Task Force Aquila, an organization the corps stood up specifically to plan and implement changes to the Marine Corps Enterprise Network (MCEN), particularly ones that'll have implications for units that will need connectivity at the tactical edge.

A big part of the task force's work up to now, in partnership with labs across the Department of the Navy (DoN), has been to model and simulate how certain pieces of network infrastructure and design choices would behave under various conditions. But those simulations have some big constraints:

It's tough to test the hardware you would use in a theoretical scenario when you don't have a digital model of how that hardware would behave in the real world.

Marine Corps leans into software-defined networking

That's one big reason the Marines want to move toward software-defined networking and infrastructure as code as quickly as possible.

"All of our infrastructure right now is purpose-built hardware. You've got one piece of hardware that's a router, another one that's a firewall, another one that's a switch," said Keegan Mills, Task Force Aquila's acting director. "What we need in the future is agnostic hardware whose function is defined by a piece of code. The vision is the code could be written on the fly – and in a very sci-fi world that looks like artificial intelligence – you'd have a network that is constructed for a very specific purpose that may only exist for a very short period of time."

In theory, not only could those elements of network infrastructure be quickly constructed and then

“What we need in the future is agnostic hardware whose function is defined by a piece of code. The vision is the code could be written on the fly. ... You’d have a network that is constructed for a very specific purpose that may only exist for a very short period of time.”

– Keegan Mills, Acting Director of Task Force Aquila, Marine Corps

vaporized depending on actual battlefield needs, but using an architecture that works along those fundamental lines would make the modeling work the task force is doing right now a whole lot easier.

Will the digital twins concept eventually take hold?

For a while, a few years ago, the Navy and Marine Corps saw a huge amount of promise in the concept of digital twins – the idea that systems could be designed based on accurate digital models of how individual components’ physical counterparts work in the real world.

But it turned out that even when sea services are working with purely IT systems, the digital twin idea doesn’t work as well as envisioned – at least not yet.

“The term isn’t used as much now as it was a year ago. And one of the reasons is it’s like an onion: You start peeling back the skin and just layers of complexity, and we’ve kind of hit the limits of the technology that we have available to us,” Keegan said.

“It’s my personal belief that to have a meaningful digital twin, we really need to have code-defined infrastructure. We’ll make [the twin strategy] more useful when we have code-defined infrastructure.”

Thinking about naval networks as pieces of code instead of specific cables connected to specific boxes opens up a lot of other possibilities, including when it comes to how the sea services secure their information, said Jane Rathbun, DoN chief technology officer.

“We want to shrink the attack surface and not necessarily have all of these networks defined based on the classification of the data that’s going to ride on them,” she said. “Instead, I can differentiate the risk of the loss of data from the environment. We also have to be thinking about the amount of money we should be spending on IT, and it certainly isn’t true that we should create a physical network for every use case. We have to get away from that thinking and move to this kind of idea.”

Standing up software-defined networks when & where needed

In fact, the broader department has already started to do some of that work, at least on a conceptual basis.

The Marine Corps argues it’s already done most of the work of collapsing the preponderance of its IT infrastructure into the single MCEN construct, even if it’s not literally true that every single piece of the network is interoperable and cohesive.

The DoN is trying to embrace that way of thinking, for at least the near term, too. That’s a departure from as recently as two years ago, when the department’s goal was to use the latest competition of its Next-Generation Enterprise Network (NGEN) contract to collapse its overseas and U.S.-based networks into one.


Instead, the current idea is to let the existing menu of naval networks operate as they do today but pay much more attention to practices that would let those networks be managed as a single “logical” network.

The name for that tall order is LUNA, short for Logical Unified Network Architecture. It aims to tie together the various connections between the Navy's U.S.-focused Navy-Marine Corps Intranet, its overseas OneNET, its Consolidated Afloat Networks and Enterprise Services (CANES) networks and MCEN, into a single, manageable design concept.

"The Navy has a certain view of its networks: That there's a geographic boundary and a functional boundary that it never exceeds, and it only has to do things in that environment," said Chris Morris, who's helping to lead the LUNA effort from the DoN CIO's office. "The Marines have a different idea about their network, which is that we're going to train and recruit, and build, run and fight on the same network all the time. But we're a naval enterprise, and fleet Marines have to get on ships."

Cross-network functionality all the way to the edge

The challenges, Morris said, are mostly around discerning how much commonality currently exists between the networks, what commonality needs to be created and the extent to which each element really matters to the bigger naval enterprise. "LUNA is not a call to action to collapse all networks into one. It's a call to action to figure out how common those things can be and how common

those things must be to allow the development and delivery of warfighting capabilities everywhere they're needed in the minimal size possible," he said. "Currently, an aircraft carrier has about 50 megabits of bandwidth while it's underway, and that's great compared to where they used to be. It was a couple of megabits. We also have to think about when it starts losing connectivity to the things that it needs to communicate with on shore or to remain completely quiet. Those are all the things we're trying to express in the design concept. What has to be similar and different about all of these different networks in order to allow developers to develop and deliver capabilities to those networks that actually work?" 

"It certainly isn't true that we should create a physical network for every use case. We have to get away from that thinking."

— Jane Rathbun, Chief Technology Officer, Department of the Navy



Air Force builds on incremental ABMS improvements, ready to expand program



BY SCOTT MAUCIONE

This spring, the Air Force brought in lawmakers to witness the latest developments of its Advanced Battle Management System (ABMS).

The tour included the Shadow Operations Center-Nellis, a laboratory that is identifying emerging technologies for faster data transfer to service members.

"The Shadow Operations Center is critical to the Air Force's drive to link information to sensors and shooters in real time," Air Force Chief of Staff Gen. C.Q. Brown said. "As our service continues to accelerate change, the revelations coming out of this battle lab will help our warfighters more quickly understand, share, decide and act, which will provide them a greater advantage on the battlefield."

The Advanced Battle Management System is just one part of the Defense Department's Joint All Domain Command and Control (JADC2) program that will deliver information, weapons and precision to the battlefield.

"DoD uses ride-sharing service Uber as an analogy to describe its desired end state for JADC2. Uber combines two different apps: one for riders and a second for drivers. Using the respective users' position, the Uber algorithm determines the optimal match based on distance, travel time and passengers (among other variables)," the Congressional Research Service report on JADC2 noted. "The application then seamlessly provides directions for the driver to follow, delivering the passenger to their destination. Uber relies on cellular and Wi-Fi networks to transmit data to match riders and provide driving instruction."

JADC2 will ingrate that cloud environment to share satellite images, intelligence and other data across networks in the same way to help commanders and service members make decisions faster.

The military wants to integrate artificial intelligence to quicken response time by using algorithms to identify targets.

Building the heart of JADC2

ABMS is critical to the command and control aspects of JADC2. The program is using the Air Force's Cloud One architecture to link sensors and weapons systems for JADC2. That includes information collected by drones, planes, people on the ground and even robots.

To keep systems connected in a degraded environment, the Air Force intends to create an internet of things approach.

One concept uses KC-46 tankers as hotspots to offload data to jet fighters as they refuel.

"Nearly two years of rigorous development and experimentation have shown beyond doubt the promise of ABMS," Brown said. "We've demonstrated that our ABMS efforts can collect vast amounts of data from air, land, sea, space and cyber domains, process that information and share it in a way that allows for faster and better decisions. This ability gives us a clear advantage, and it's time to move ABMS forward so we can realize and ultimately use the power and capability it will provide."

The Air Force uses on-ramp tests to bring in new technologies to the ABMS fold. Those tests have brought in partner nations, integrated robot dogs and hooked into SpaceX's Starlink system.

"Nearly two years of rigorous development and experimentation have shown beyond doubt the promise of ABMS."


– Gen. C.Q. Brown, Chief of Staff, Air Force

"The Navy's doing something similar for their overmatch program for their JADC2 approach. We think that's a pretty good model. We're probably going to do something that looks a little bit more like that."

– Air Force Secretary Frank Kendall

As ABMS progresses, service rethinks tech organization

The Air Force is also thinking organizationally about ABMS. Air Force Secretary Frank Kendall said the service is rethinking its chief architect position in terms of bringing together technologies.

"We need to create something that has more that kind of responsibility of tying things together," Kendall said of the chief architect position. "I haven't even decided what we might call it yet, but we want to move in that direction. The Navy's doing something similar for their overmatch program for their JADC2 approach. We think that's a pretty good model. We're probably going to do something that looks a little bit more like that." 

Army kicks Unified Network Operations effort into gear



BY JASON MILLER

Maj. Todd Donaldson, a communications and network officer for the 2nd Armored Brigade Combat Team, 3rd Infantry Division in the Army, has a simple request when it comes to network modernization.

“At the operational level, I just want to be able to see my network, both the upper tactical and the lower tactical, especially as those mesh radios have been integrated into the formations,” Donaldson said at the recent Technology Exchange Meeting (TEMS) hosted in Philadelphia by the Army’s Program Executive Office Command, Control, Communications-Tactical (PEO C3T).

“I want to be able to see what’s on the network, what’s not on the network,” he continued. “If something starts to drift, I want to be able to pull it back in. I want to be able to see how much data we’re using and how congested that network might be at that time. I want to see how many users we have up on it as we continue to expand with our mesh network, and I’m going to have a lot of radios on that network. I need to be able to see it, and sometimes it feels like we’re very much flying blind. But to be able to see that would really help me enable and facilitate that capability for my commander.”

Donaldson’s summation of the Army’s straightforward desire is what’s driving the Unified Network Operations (UNO) strategy over the next six years.

The [Army Unified Network Plan](#) outlines the high-level journey the service began last year and that will pick up steam in 2024 when UNO becomes a program of record.

“The Army Unified Network employs a common operating environment, services infrastructure and transport layer, as well as unified network operations and cyber defensive capabilities. It enables intel at all levels of network classifications required to conduct multi-domain operations,” the strategy stated.

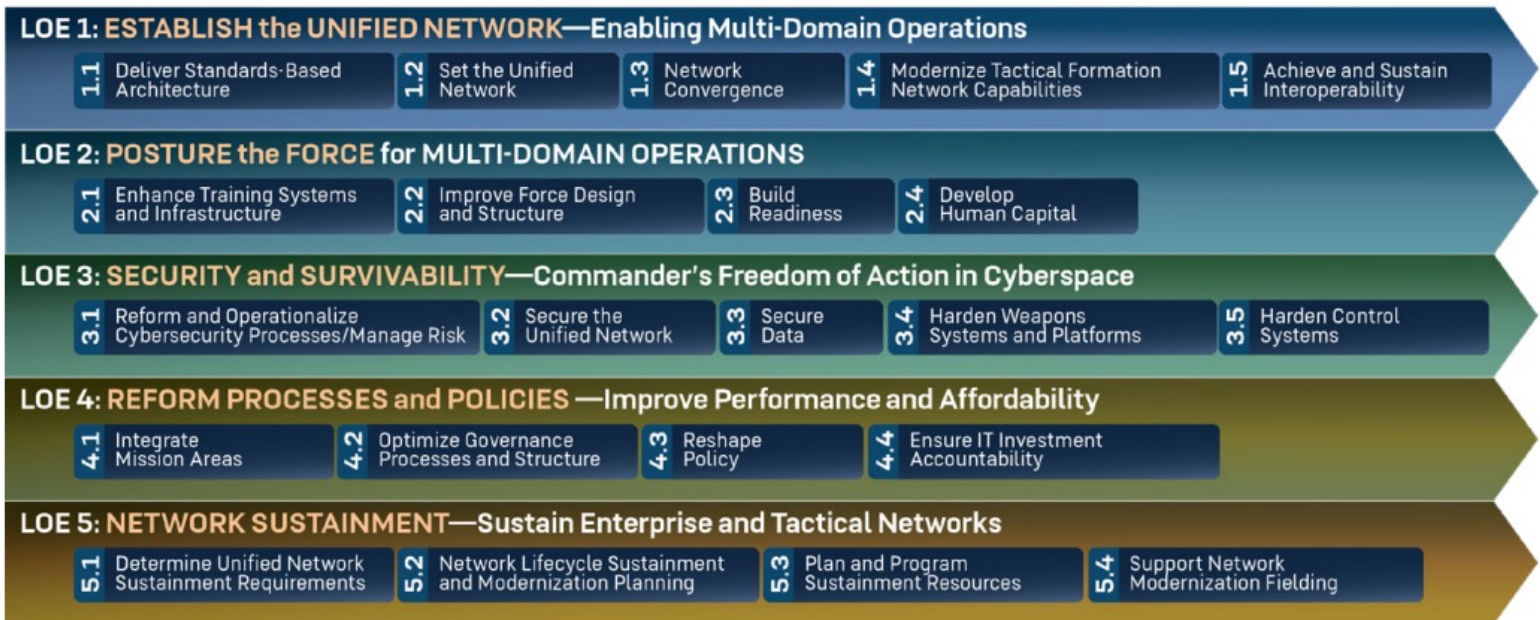
The plan details five lines of effort (LOE) that will shape UNO and lead the Army toward multidomain operations by 2028.

Army Chief Information Officer Raj Iyer said at the event that the strategy is turning the service’s network modernization approach on its head. Instead of putting the network above all, the data and the fabric that underlies the data is driving the service’s approach, Iyer said.

“How we’re architecting the unified network for the future really is to start with the data first, and then we put the zero trust cyber architecture on top of that because, again, that cannot be an afterthought,” he said. “So once you do those two core pieces, the rest of the network now starts to flow, quite frankly, a little easier because now we’ve made those decisions on what level of data we need – where, when and how much – and how much of that needs to be in a disconnected mode in a digital environment versus persistent connectivity back in some sense.”

Iyer summed up the projected end state of UNO succinctly: “At the end of the day, the network has to be scalable, resilient, secure and survivable because we know with a near-peer adversary in the future, one of the first things that will happen and, we validated

Army Unified Network Plan Framework



Source: Army, "[Army Unified Network Plan](#)," 2021

this most recently in Europe, is electromagnetic warfare, and the first thing that will happen is the jamming of your network. So how extensive do you want this to be? How can you get to this mesh architecture, where you don't have a single point of failure in the architecture? Because today, that's how we operate."

Acquisition strategy coming into focus

The October 2021 strategy was the first step, but now the Army is moving into the acquisition and implementation stages of the effort.

Making UNO a program of record in 2024 will ensure the Army funds and tracks its progress.

The acquisition piece is starting to coalesce too, with an initial request for information from the Army's Program Executive Office Enterprise Information Systems (PEO EIS) this summer and then a draft request for proposal in early fiscal 2023. The Army expects to release the first of several expected solicitations for UNO by June 2023, with an award by December 2023.

"Right now, we're thinking about merging upper and lower tiers into the same contract and maybe figure out is there a way where we can get after solutions that support IT support both within a command post and between command posts?" said Matt Maier, the Army's program manager for interoperability, integration and services within PEO C3T.

"The question is, how can we bridge that enterprise identity and access management capability down into the tactical space? We need to do that by merging and collapsing of capabilities. But it's likely to be a different type of a vendor approach for us, and we'll probably use some different vendors' capabilities. So, that may end up becoming its own separate contract vehicle."

No matter how many requests for proposals end up coming out, the end result has to come back to Donaldson's request to simplify and reduce the burden on soldiers and commanders, Maier said.

"We want to reduce the cognitive load for them. We want to reduce the time it takes for them to complete tasks. We want to provide that single pane of glass, and we want to provide that common user interface. We want it to be simple, easy and as intuitive as possible to use," he said.

“I think that capabilities to apply both at the tactical space and the enterprise space is going to require close collaboration between multiple program managers. We’re going to have to develop some kind of standards that everyone would have to conform to so that we can merge them together. We’ll probably be developing an application program interface. We’ll definitely be producing some API middleware for you to use, which will allow you to build capabilities that can fall within this construct and conform to the single pane of glass graphic user interface that we want to provide to soldiers.”

Requirements under review

Sometimes industry partners will design technology for a radio, but then have to scale it across the entire enterprise to work at regional hubs and beyond. Maier noted that the software will have to be flexible enough to take on new and emerging technology when needed and available.

“The six requirements definition packages will come out in priority order. The very first one that will be signed by the Army Requirements Oversight Council this year is for the lower-tactical tier, and that happens in fourth quarter. That’s our focus in the near term,” he said.

“We can focus on what planning, management, configuration, initialization, control and monitoring tools exist today and where can we gain some opportunities for optimization. What are the building blocks that we can set the stage with for radio management, for example? Then, we can start to migrate those capabilities up into the upper-tactical tier and merge and replace older capabilities as newer capabilities come online. I think the reason that we’re starting in the lower-tactical tier and upper-tactical airspace is because capabilities there are not very well integrated, like they are in the enterprise space.”

For the Army, the lack of integration and duplicative, noncomplementary capabilities is a driving factor of UNO as well.

Col. Christian Haffey, director of the Cyber Capability Development Integration Directorate at the Army’s

“I want to be able to see what’s on the network, what’s not on the network. ... Sometimes it feels like we’re very much flying blind. But to be able to see that would really help me enable and facilitate that capability for my commander.”

– Maj. Todd Donaldson, Communications and Network Officer, 2nd Armored Brigade Combat Team, 3rd Infantry Division, Army

Cyber Center of Excellence and Future Concepts Center, said the enterprise network currently has hundreds of tools and capabilities that are not integrated, which are complex and costing the Army a lot to sustain.


“We’re looking to drive down the number of tools and the sustainment costs. It’s not that we’re trying to lower our investments in the network. It’s just we have to continually assess our budget, and we have to look across all areas,” Haffey said. “As we’re investing and equipping new tools, we also have to then forecast what we have to invest into sustainment and what we have to invest in training of individuals. There’s a tail of costs that we have to continue to consider.”

Network as a weapon

Part of the UNO strategy also is to identify and mitigate capability gaps on the network and in services that support the network, he said.

The long-term goal for this entire UNO initiative is to change the way the Army thinks about and uses its network.

“UNO is going to enable the Army to use its network as a weapon system. So rather than fighting against the network, as you all have done as you move from one area of responsibility to another AOR, you really fought our own network because of our own policies of our own tools,” Haffey said. “The unified network is to change that mindset, and it give us an end-to-end visibility to be able to sense, control and visualize devices and users on our network. UNO will provide that tailorable and scalable DoD Information Network operations that we will be able to tailor for that user or for that warfighter, as he or she moves across the battlefield or as he or she moves from the continental United State to Joint Base Lewis-McChord and into the Indo Pacific AOR.”

That’s the ultimate deliverable, Haffey said:
“They’re not fighting against the network.” 

“UNO is going to enable the Army to use its network as a weapon system.”

– Col. Christian Haffey, Director, Cyber Capability Development Integration Directorate, Army



'Purposeful innovation' should drive DoD network modernization efforts



Lamont Copeland
Director of
Federal Solution
Architecture, Verizon

Nearly 30% of Defense Department facilities have exceeded their lifespans, points up a [recent report](#) from the Government Accountability Office. But a military base is more than just bricks and mortar.

One of the biggest challenges DoD faces with its aging bases is

their networking capabilities. Bases built 50 or more years ago didn't anticipate the power, cooling or wiring requirements of today's technology – to say nothing of bases built during or shortly after World War II that are still in use.

But GAO also noted DoD has a massive facilities maintenance backlog, and upgrading old bases may be expensive and difficult. Some are even national historical sites, further complicating matters. That presents a major challenge to DoD's modernization efforts.

"DoD wants to get to the next generation of network infrastructure. They want these next generation infrastructures to support the warfighters' ability to do virtual training, support tactical communication networks, utilize autonomous vehicles, and also technologies like digital twinning within a shipyard or an air fleet so they can actually start working on things in a more real-time and autonomous fashion," said Lamont Copeland, director of federal solution architecture at Verizon.

"To reach these goals they need to upgrade their networking capabilities in a way that is simple to consume and purposeful," Copeland continued. "Network infrastructure changes can range with various difficulties based on the nature of the facility. Assessments need to take place to find the right combination of technology – wireline and wireless – to support the current needs of the mission but have the flexibility to support growth of the mission."

Advantages of wireless

That's where wireless technologies come into play. Setting up 5G on a base can help accelerate modernization far beyond the pace of actually laying fiber. And then once that 5G infrastructure is set up, it's easier to tie it to edge computing and begin standing up "smart base" applications like augmented and virtual reality training and autonomous vehicles, Copeland said.

5G can also facilitate the use of new technologies that rely on high-speed and low-latency networks. Though large data use applications and facilities would still require direct fiber connectivity, 5G can help lessen the need for an extensive fiber upgrade.

It's also an important factor in technological parity across DoD because the age of a base isn't the only thing affecting its capacity for modernization. Its location can be a factor as well. Urban bases tend to have more advantages regarding infrastructure than more rural, austere bases including increased access to public and private services.



David Rouse
Director of Defense
Sales, Verizon

“You’re going to see more innovation, more companies bringing a lot of capabilities out to rural areas. It’ll take time to get there, and it’ll take time to kind of do a lot of those changes that the government may want to do. And so the question is, how do we bring that parity

between urban and rural because they have the same aging infrastructure? They have the same needs as well: to be able to innovate and keep the military at its elite status,” Copeland said. “These new technologies – how you’re delivering the wireless, how you’re delivering the edge computing – will help them accelerate that innovation across bases in more rural and urban settings.”

Over the past several years, technology evolution has been the primary catalyst for infrastructure upgrades, said David Rouse, Director of Defense sales at Verizon. They’ve largely been driven by network efficiencies and equipment obsolescence.

“More recently and in some areas, there is a new driver. We are seeing local mandates and regulations about carbon footprint and green energy initiatives where legacy time-division multiplexing (TDM) and copper infrastructure is required to be shut down for more efficient IP and fiber-based solutions,” Rouse said.

Digital inclusion is another initiative with potential benefit for DoD, he said. “Improving high-bandwidth broadband solutions for rural areas where the military also has a presence presents a mutually beneficial opportunity.”

And that parity is important not just to modernize at the same pace but to standardize across DoD for training purposes too, Rouse said. As an example, warfighters may need to be able to pick up a network at one base, transfer out their connectivity to a different base, and have all their credentials and experience seamlessly transferred so that they can pick up right where they left off.

Enterprise visibility

A better network foundation and standardization also gives the services visibility across all of their platforms and capabilities. By having a consistent underpinning for communications and compute paths, DoD is helping lay the foundation for consistency across apps and services as well. It also can make enterprisewide security easier. Aging technologies that may have less updated patches and enhancements could have a lot of inherent security flaws that introduce vulnerabilities into network environments,

“The question is, how do we bring that parity between the urban and rural because they have the same aging infrastructure? They have the same needs as well: to be able to innovate and keep the military at its elite status.”

– Lamont Copeland, Director of Federal Solution Architecture, Verizon

Rouse said. Having that visibility makes it easier to flag anomalies and potential intrusions.

But DoD also needs to bring these capabilities to its operations outside the continental United States. And that's a challenge because DoD can't take advantage of the national infrastructure it has in the United States, he said.

"Foreign countries sometimes incorporate technologies in their infrastructure that are produced by near-peer adversaries, which may be restricted for use on U.S. installations as per the National Defense Authorization Act," Rouse said. "Base personnel are mitigating risk at the demarcation points where base connectivity meets local connectivity. Private wireless can selectively be leveraged for foundational connectivity based on the location of the base." But it's equally important to avoid the potential pitfall of technology for technology's sake, Copeland cautioned.

"We need to understand how all the vendors are bringing in technology to drive that mission set. We're purposefully trying to innovate and modernize all these different bases and different facilities to meet that goal," he said.

"There are a lot of really good technologies and services out there. But the question is, how to make sure that we are driving a purposeful innovation to meet the specific goals of the military?" Copeland added. "The way to get there is making sure that we're partnering well with the government to understand what their needs are." 🤖

"More recently and in some areas, there is a new driver. We are seeing local mandates and regulations about carbon footprint and green energy initiatives where legacy time-division multiplexing (TDM) and copper infrastructure is required to be shut down for more efficient IP and fiber-based solutions."

– David Rouse, Director of Defense Sales, Verizon

Learn about DoD's effort to modernize and evolve toward the smart base of the future in this Federal News Network ebook, *Anatomy of a 5G Smart Base*, in partnership with Verizon.

[**Click here**](#) to read it now.