Government Business Council

Expert Dialogue

TRANSFORMING THE NETWORK ON AND OFF THE BATTLEFIELD

5G AND THE DEPARTMENT OF DEFENSE

Underwritten by: AT&T

Introduction

Securing America's networks does not stop at America's borders. Maintaining the tactical edge also means security at the edge, a transformational shift away from traditional methods of security to a new world of zero trust and 5G technology. The Department of Defense has made significant investments into this technology that will enable them to maintain domain command and control. With these investments, what does the future of network security look like on the battlefield and at home? To find out, Government Business Council spoke with some of the Department of Defense's top IT experts about the greatest threats facing the DOD, and what is on the horizon for their agency.

Experts

Dr. George Duchak
Chief Information Officer, Defense Logistics Agency

Jody Little
Executive Program Manager/Director, USAF Joint Base San Antonio 5G NextGen

Paul Puckett
Enterprise Cloud Management Office Director, U.S. Army

What do you think are the greatest network security threats that the DOD, and your agency in particular, is facing today? How is the DOD responding to these threats?

Puckett: One of the biggest challenges is that our workforce and our workloads are becoming more distributed globally. This movement from known, physically owned endpoints to an unknown and software-defined world is spreading our resources from how we've always addressed, seen, and secured our network into being able to operate and defend in real time. The simple vignette of COVID: Overnight, we had to maintain mission; move everyone to their homes, which no one's done a physical inspection of; move everyone to, for the most part their personally owned devices, which there's no device management of; and yet still be able to operate and defend and support the mission of the United States Army.

> "The convergence of those elements—of this legacy world, this new world that we have to operate in, and the threats from all angles—is becoming a perfect storm that's driving a sense of urgency to adapt and address it in real time."
>
> **- Paul Puckett**

The biggest threat is just this changing landscape. A lot of the systems that are currently operating our mission today were designed with the kind of security in which we trust everything. We see this need to move to this distributed world, this zero-trust world, but all of the operational capabilities that we have today were never designed or configured for it. Now I've got these two worlds that were probably never meant to work in the same space trying to work together. Add in rogue actors who want to sow distrust and chaos, by inserting themselves in the middle, because there's potentially a dollar to be made. The convergence of those elements—of this legacy world, this new world that we have to operate in, and the threats from all angles—is becoming a perfect storm that's driving a sense of urgency to adapt and address it in real time.

Little: We realize there's a lot of threats, both from foreign nations and malicious standalone actors. If we don't secure them up front, there will be gaps that will allow leaks and penetrations. The response is to move to the front end of this, but securing the internet and DOD specifically is a big challenge. If we do our job right in DOD over these experiments and over this period, it can improve security.

The OUSD (R&E) [Office of the Under Secretary of Defense for Research and Engineering] 5G enterprise is working hard to get DOD ready. We've got a lot of initiatives to get there, and Congress was smart about doing that. Rather than allocating a lot of funding in [research, development, testing and evaluation], they opted for prototyping, which means they were able to build working capabilities with transition paths. That forces you to address issues that you might not have seen in a typical R&E initiative. There's a number of good experiments going on, focusing on different areas like spectrum and augmented reality, but we're all concerned about the security of those devices.

Duchak: Some of the greatest security threats are cyberattacks, malicious actors, phishing attempts and exploited vulnerabilities. For the Defense Logistics Agency, we are continuously looking for ways to fortify our information networks and business systems by reducing vulnerable points where an adversary could gain access and move across and within our networks. Some examples include using hardened devices, managing software patches and reducing our attack surface.

> "Some of the greatest security threats are cyberattacks, malicious actors, phishing attempts and exploited vulnerabilities."
>
> **- Dr. George Duchak**

We remain vigilant in our security focus through a comprehensive Cybersecurity Operations Division, which not only includes a 24x7 Computer Emergency Response Team, cybersecurity vulnerability managers and embedded counterintelligence capabilities, but also now includes an Assured Logistics Cyber Center. This center will help us stay ahead of threats to the logistics supply chain by aligning DLA's critical business functions with cyberspace operations to proactively identify strategies and techniques to address risks and plan for mitigations. We recognize the importance of integrating cybersecurity into daily business operations, including our software, hardware and supply chains. DLA is adopting this model in its hosting strategy and cloud environment to minimize risk and introduce industry best practices.

Zero trust is a priority in cybersecurity policy throughout the DOD. What is your agency doing to implement zero trust?

Duchak: Zero trust architecture is something the federal government is very focused on right now, as it should be—it enables cyber analysts to think beyond the perimeter security mentality, including the unit of control for cybersecurity, which has traditionally been the IP address. We would build perimeters or moats to keep out certain IPs and let in others. With zero trust, the IP is replaced by identity as the unit of control or trust. It's based on the idea that organizations need to proactively control all interactions between people, data and information systems to reduce security risks. This means we need to verify the human, the machine, the connections between machines, between humans, and between humans and machines. So, while the typical network-centric approach to cybersecurity generally assumes that users inside a network can be trusted—in the zero-trust security model, users and devices both inside and outside the network are, by default, considered not trustworthy. Therefore, it continually assesses, authenticates and authorizes access which enables our defenders to find and remove adversaries from the network.

> "We recognize that zero trust isn't some sort of appliance or application you place on your network. We know it's more about a mindset change."
>
> **- Dr. George Duchak**

For DLA, we recognize that zero trust isn't some sort of appliance or application you place on your network. We know it's more about a mindset change. We are currently enmeshed in a significant digital-business transformation—the first one in more than 20 years—that is enabling us to rethink our business model, our value proposition and with that, our business processes. Part of our modernization effort is to implement the zero trust strategy which embraces those tenants to build secure software in our DevSecOps software factory from the start. This includes re-platforming to a single sign-on user persona that automatically limits where a user can traverse on our network while giving the right user, the right access, at the right time.

Little: When people think of zero trust, they think of cybersecurity, locking out and authentication, but a lot of things go into that framework. You're looking at different areas inside the ecosystem, from the cloud all the way out to securing the edge. For example, there's a lot of devices now with 5G that have dual radios. If I'm tied into a secure slice, let's say classified collateral, and I have access to the internet, there's an ability for crossover there. I have to be able to secure my UE [user equipment] as well. While we're not heavily focused on the UE here, we do have a big concern about that and we're working with others.

How is your agency managing and securing edge devices (i.e., smartphones, tablets, hotspots, laptops and IoT)?

Puckett: A lot of the challenge of securing edge devices, not only from an identity perspective but also from a secure configuration perspective, is how we've been doing it for many years; typically well locked down, least-privileged access, numerous components monitoring the different configuration of systems and endpoints, applying group policies in the way that we have secured devices, and then a hyper awareness in monitoring all ingress and egress of network traffic, whether that's user traffic, data traffic, or management traffic.

The challenge is that it's typically addressed in a point-in-time fashion. What we're leaning into now is true continuous monitoring, not whether we have a given configuration. We're starting to employ tactics that make it an environment and a capability that can fix itself. Typically, when we talk about continuous monitoring, it's only monitoring. What it needs to become—and what we are doing today in a few places although not where we need—is continuous remediation. That pivot is towards DevSecOps. We can demonstrate the ability to conduct the mission and continuously remediate back to a known good state when it comes to how our edge devices and capabilities are built, configured, monitored, and secured today.

> "When it comes to cloud and edge computing, the DOD learned quite a while back that you don't build the systems and then secure them. That doesn't work well. From the start, security has to be paramount in all the programs..."
>
> **- Jody Little**

The way we conduct mission edge devices and where they're deployed today are typically untrusted physical environments. There's not a massive pivot there. The pivot is when edge devices of government furnished equipment have to connect, not to my office and the Pentagon, but to my home Internet. It changes the threat vectors. Sometimes not everyone gets government furnished equipment, yet they still have to conduct their job.

[COVID] drove home the realization that this distributed and untrusted endpoint architecture is already the new reality. Before it was seen as this very small subset of users. Now it's the predominant driver of our users. It only helped accelerate the realization and the need to lean in, not only as something else that we have to address, but also as something that can actually be transformational for how I conduct the mission, how I secure my ecosystem, and how I can expand contributors into that ecosystem. Hiring practices across the DOD are seeing this new world of defacto remote telework users on personal devices. I can hire talent that doesn't necessarily sit close to a camp, post, or station of the United

States Army. It's been a positive opportunity for recruiting that also enhances the way we look at security.

Little: When it comes to cloud and edge computing, the DOD learned quite a while back that you don't build the systems and then secure them. That doesn't work well. From the start, security has to be paramount in all the programs, in order to secure the 5G systems as they come into DOD. It plays a huge role across all of the tranches and the operate-through programs. This means looking at how we can take programs and put them in military applications, whereas the tranches are building capabilities that will transition into military applications. When we say operate through, they've got to operate securely and reliably. As we coined the phrase here, secure and trusted 5G. The multi-edge computing capability of 5G takes software and puts portions of it in the edge. Other portions are in the cloud running other applications. It brings significantly more capability, but it's also going to bring orders of magnitude in terms of volumes of data and low latency. Instead of securing an IoT [internet of things] device, I've got to secure an IoT device that can go into operations.

> "From the start, security has to be paramount in all the programs, in order to secure the 5G systems as they come into DOD."
>
> **- Jody Little**

Duchak: Under normal conditions, DLA has about 7,000 external connections with edge devices. With mass telework related to the COVID-19 pandemic, those connections dramatically increased to more than 25,000. A major part of our solution is the use of a Virtual Private Network, which minimizes the risk associated with end-point devices as vulnerable vectors for attack. We can ensure the VPN infrastructure is secure, and at the same time continue to make upgrades to our systems to reduce latency and provide the best user experience possible. For devices that need to be connected directly, we continue to harden them per a secure baseline and ensure they are patched, encrypted, and secured with multi-factor authentication.

Another avenue for managing and securing our edge devices is to use the Defense Information Systems Agency's solution: a government-owned, secure credentialing process for mobile devices which provides over-the-air derived credentials to more than 100,000 Department of Defense-issued commercial mobile devices. DISA's purebred technology provides us with the technology needed to secure our mobile devices while continuing to access the DLA network.

How can partnership between the private and public sectors affect DOD cybersecurity and mission?

Puckett: Software and data truly run the world. We're working on how we incorporate our ability to see our software bill of materials. It's really critical that, in our partnerships, they have the actual bill of materials when it comes to the software that they deliver to us. Take the 5G physical supply chain. The national security implications when it comes to our ability to have access to commodity compute and storage that does not have influence from adversaries of the United States is a very, very real challenge. The Army has been leaning in heavily to ensure from a compliance and a contractual perspective that we're partnering and working with vendors that are able to provide a high level of assurance and confidence, so that we know the origins of our capabilities. We are constantly monitoring what our adversaries are doing with technology and where we could be vulnerable. We are also considering how we need to address those vulnerabilities in the physical supply chain.

> "Open source is fundamentally transformational when it comes to access to great software technologies and ideas. But how we package that up together to deliver it as a capability and continuously enhance versions of our services is really critical."
>
> **- Paul Puckett**

Far too often, we've acquired these capabilities that are seen as a black box of technology. From a software perspective, what are the open-source components that you're compiling? There are so many vectors when it comes to threats in the software supply chain. Every day you see in the news that people are exploiting open-source software. It's a different type of capability and technology that we have to address in a different way. Open source is fundamentally transformational when it comes to access to great software technologies and ideas. But how we package that up together to deliver it as a capability and continuously enhance versions of our services is really critical. That becomes a real time information sharing challenge.

I'm thankful for the Cyber Executive Order that includes the software bill of materials. We need to be sharing openly with our industry partners, because we have to be mindful of the life cycle of each of the components and capabilities. We have to ensure, from a national security perspective, that we aren't leaning heavily into a technology that could have immense vulnerability implications of influence from another government that perhaps has some adversarial views of the United States and our mission.

Little: One of the big challenges is that, for this to work, we have to have partners. Most of the big program work experiments are awarded via OTA [other transaction authority]. We have about 12 different industry partners in these OTA experiment programs. That's a lot. We went with a single award prime because we have to push towards transition and making these things work fast. DOD telemedicine needs this. This is going to save lives; this is going to extend the future of DOD medicine. The same thing is happening on the commercial side.

For example, in training right now, trainees have to come to the trainer or the trainer goes to the trainees. If I've got a doctor or a medic or a nurse in the field who's not a specialist, I can in real time reach back and find that expert at base, who would be able to see exactly what the medical staff is seeing in the field. You can get the right expertise when it's needed into the field, including neurosurgery or cardiology. Another project that we're working on takes tele-mentoring into the austere environments, meaning field and emergency medicine, where you have medics on the ground. They call that the golden hour, where they can get the patients to the right experts to save their lives. They'll be able to use AR for massive training either directly with multiple students in multiple places or even with single students, or they could allow students to train somewhat on their own. It brings a lot of capability that can be extended around the world, if you do it securely.

> "A multi-cloud strategy can be beneficial for many reasons and when coupled with a hybrid-cloud solution, the cybersecurity capabilities can be even greater."
>
> **- Dr. George Duchak**

Duchak: DLA continues to actively engage internal stakeholders and external partners in maintaining a persistent state of cyber-situational awareness and preparedness. A few years ago, DLA began leveraging commercial cloud offerings to help reduce infrastructure and duplication. This collaborative effort between the private and public sector promotes competition and ensures reliability and security in the cloud.

We embraced a multi-cloud strategy to provide DLA with advantages in preventing data loss and avoiding vendor lock-in, redundancy and price-competitive services. Not all clouds are created equal, and a multi-cloud strategy offers DLA the ability to select different cloud service providers based on the services, capabilities and features that are the most suitable for an application. A multi-cloud strategy can be beneficial for many reasons and when coupled with a hybrid-cloud solution, the cybersecurity capabilities can be even greater. DLA is committed to realizing the value of cloud computing to provide a secure enterprise computing environment.

How does your agency envision balancing the requirement of isolated private 5G networks and the need for connecting devices to commercial networks while roaming?

Little: 5G was intended to be able to take care of all these open devices that carriers have. That's why we have the standards. How do I take advantage of using those systems? If they're following the standards, and we deploy our zero trust and our encryptions, it should technically work on any system. For example, getting authorization to operate a DOD network with critical data on a network in an African nation that's been put in by a foreign manufacturer from China is something that's still evolving. A lot of the focus has been on running private networks, connecting to the government private clouds and extending to MECs [multi-access edge computing]. You're going to have that in a lot of places because of the mission. For day-to-day base operations, network slicing becomes important. I can set up a slice that carries the military traffic and leave other slices open for the commercial traffic. Right now, you have to tunnel through, and you may not have the capacity. But 5G will provide that.

Slicing, encryption, and all these other cybersecurity features that are available will support that capability, but it still remains a work in progress. Ideally there are applications at different levels that you would like to run securely. We'd like to be able to go to a host nation and operate over the same system as we have here in the States. That's where interoperability comes up—not only being able to interconnect, but to do it securely.

There are a lot of functions in edge computing that you can accelerate, while keeping the backhaul smaller. We like to think about deploying 5G bubbles—secure bubbles that are supporting the UE and can move with the troops. Then my backhaul can be done other ways, whether it's through satellite, a commercial line or some other means. You can connect your base station to fiber optic somewhere. For tactical purposes, you have to allow for different contingencies.

> "We like to think about deploying 5G bubbles–secure bubbles that are supporting the UE and can move with the troops."
>
> **- Jody Little**

Duchak: The 5G ecosystem runs the risk of exposing DOD systems and networks to malicious security vulnerabilities just as every other new technology we've embraced. It can, however, also offer enhanced services, everything from improved wireless speeds to sharing large amounts of data in real time. With that risk and reward understood, we are looking into several mitigation strategies, including how we can architect topologies based on the two deployment formats. We also envision balancing the requirement through service-level agreements signed between private 5G networks and commercial 5G networks, so that devices will be able to roam between the private and commercial networks based on the

> “We’re moving more and more into a software-defined world. Our ability to compete and win with software is enabling our ability to commandeer and leverage any single physical medium possible to conduct our mission globally.”
>
> **- Paul Puckett**

credentials provided on the SIM card. That is in addition to ensuring the devices are secured per previously mentioned methodologies.

Puckett: For any physical infrastructure that we use – any medium of transport and connectivity—there will come a point where we’re not able to physically inspect every single environment or physical space that we use. There are so many commercial services that we use globally. Our ability to encrypt and overlay our mission on the move—our ability to leverage any means and mechanism of transport and truly be transport-agnostic when it comes to conducting our mission, our ability to pivot from 5G to LEO to fiber—that flexibility and adaptability overlaying our security is transformational.

At that pivot point, what medium is available that is a potential asset for me to leverage to the greatest extent possible? I’m not concerned whether defense security service has inspected their physical space. We’re moving more and more into a software-defined world. Our ability to compete and win with software is enabling our ability to commandeer and leverage any single physical medium possible to conduct our mission globally. That’s a critical movement for us to be able to leverage any physical infrastructure when and where we need it.

Indsutry Perspective

Rita Marty | Vice President of Security Architecture, AT&T
John M. Dillard | Director, DOD 5G Strategy and Solutions, AT&T

What do you think are the greatest network security threats that the Department of Defense (DOD) is facing today, and how can AT&T work with them?

Rita Marty: Cyber threats are increasing both in frequency and intensity across the whole ecosystem, whether it's the private sector or the defense space. While the DoD is especially at a high risk for cyberattacks, they have begun to take advantage of commercial technologies that can help them keep pace with near-peer adversaries, who have been rushing to adopt and deploy technology for military missions.

There are, however, two factors that are putting the DOD at greater risk: First, the DOD should invest more in industry models like the Enterprise IT as a Service (EITaaS), which offers the military an overarching network operations framework that can provide critical network visibility and the ability to enforce compliance. Second, without an enterprise procurement and operational delivery model, the DOD is more vulnerable, due to the seams that exist within legacy infrastructure. These become attack surfaces that adversaries can easily penetrate.

The pandemic has also had a considerable impact on DOD operations, as personnel had to adapt to working from home. Many realized that they have better network performance at home than at their work sites or on military bases. With this fact in mind, the DOD should examine and update policies to allow more commercialization of on-base networks, like the EITaaS model, which would provide a secure and high performing network infrastructure.

Let me pivot to 5G: For the DOD, the capabilities of private 5G networks can allow our military forces to manage traffic locally that may be classified, while still taking advantage of our commercial network. With computing capabilities at the edge of the network, their critical data can be kept segmented and isolated for local processing.

John Dillard: The DOD now considers their network as a core piece of warfighting architecture, which is a perspective that differs greatly from the past. They realize that they need highly secure and resilient networks that can enable artificial intelligence and data-driven initiatives.

If you consider the tactical missions and global operations from a security perspective, the DOD needs to protect any signal through the proper cyber mechanisms, so that military forces can carry out operations in radio frequency (RF) contested or congested environments. AT&T can assist the DOD in deploying these technologies through our internal cyber resources or network of partnerships and alliances.

How do you think 5G offerings from service providers might support the broader military mission on a global scale?

Rita Marty: 5G is a real game changer for the DOD. It provides higher bandwidth and ultra-low latency, as well as more density, better coverage and stronger security. As we roll out 5G technology, we embed security into our network, rather than treat it as an overlay or a standalone feature, which is what we have seen in the past. 5G is going to significantly improve the way the military operates. Capabilities such as network slicing can segment or isolate traffic from an end-to-end perspective, not just in the core, but also in the radio access network. Network slicing offers the DOD many security benefits, in terms of added protection or security controls.

5G can also push everything to the edge of the network, with ultra-low latency that will enable services that are not available today. This capability can support the DOD in mobilizing their operations, by distributing data and applications closer to where they are needed, whether it's in a command center or in the field. The distributed nature of 5G gives the DOD the option to handle data collection or analytics at the edge of the network or at a central location, at faster speeds than previously possible. 5G can support the DOD as they scale for distributed and mobile operations, as they stand up and take down command centers quickly and efficiently before detection. The ultra-low latency is also a big enabler for next generation services, such as drones, artificial intelligence and machine learning at the edge of the network.

> "5G is a real game changer for the DOD. It provides higher bandwidth and ultra-low latency, as well as more density, better coverage and stronger security."
>
> **- Rita Marty**

John Dillard: Resilient communications is a primary objective of the joint all-domain command and control (JADC2) vision for the DOD. We've been supporting Defense agencies and our armed forces as they accelerate 5G testing and deployment, including securely operating through 5G infrastructure. The mobility component of 5G can provide resilience for centralized or decentralized communications. The DOD can also leverage AT&T's investment in the EITaaS model, to gain better network visibility and enforce any security compliance required. Implementing EITaaS can also extend the wireline network into the mobility realm, which would support edge computing capabilities for war fighting operations.

How do you think 5G technology will increase the possibilities for—and positive outcomes of—collaboration?

Rita Marty: The goal is to build resilient networks and embed security into the design from inception. One of the industry forums that is gaining momentum in this initiative is the O-RAN ALLIANCE (Open Radio Access Network). AT&T is collaborating with many providers in the industry to deliver innovation not only in the core network, but also at the edge of the network, even the radio access network. We are looking for ways to disaggregate the radio access network to use open interfaces and network concepts. This would provide insight into the radio access network and therefore enable improved security, better security control and more visibility of the traffic through the edge of the network.

As we migrate to cloud architecture, including private and public cloud, encryption and DDoS protections, we remained focused on defense in depth and layers of controls. We are embedding security measures from end to end—from strong identity access management platforms to monitoring and analytics, from scanning code and network interfaces to vulnerability management and cloud security. That's the principle of our core network, as well as the 5G distributed model. The same platforms and capability can power all of this.

John Dillard: 5G open radio access network, or O-RAN, will be the key to integrating operations and implementing the DOD's vision of all domain command and control, to eliminate seams and connect the sensors on the edge into the network of networks. A multi-tiered security foundation will be critical to their global infrastructure, as we continue to build out this network at large.

What particular role do you think the private sector has in supporting the government's 5G goals, and how can advanced solutions help agencies within the DOD mobilize their missions and modernize agency operations?

Rita Marty: The private sector is innovating at speed, investing heavily in building an infrastructure on a global scale. Partnerships with commercial providers would give the DOD access to state-of-the-art technologies at a lower cost than building their own network of networks. With AT&T's global footprint in more than 225 countries, the DOD could take advantage of our vast resources, instead of attempting to duplicate the innovation that already exists. The DOD can also benefit from the layers of security controls embedded in our network and our extensive operational and security models.

We know that the DOD has global missions in Europe, Asia and Africa, which requires them to securely operate through existing infrastructures. Commercial carriers have roaming agreements with many nations, but there may be circumstances that require customization to support RF operations in DOD spectrum bands. The DOD is going to need flexible solutions to seamlessly integrate wireless and wireline networks, which would align with their vision for joint all domain command and control, or JADC2. Adopting secure, open architecture would enable this vision and expedite the adoption of 5G technology.

John Dillard: As a global provider, AT&T can deliver end-to-end solutions for the DOD's tactical operations, with security at the foundation of everything we do. We're currently engaged with the DOD on many 5G opportunities that are customized solutions. We have adapted 3GPP standards-based solutions to meet many of the DOD capability sets, and we're building prototypes that support DOD goals, including smart warehouses, AR/VR and even tactical 5G solutions.

We've been heavily involved in thought leadership for dynamic spectrum sharing, which is at the core of what we do to provide mobility and wireless services. We're adapting capabilities from our commercial segment for the DOD and gaining insights from the process. We're in lock step with the DOD, moving faster to adapt to the way they must combat their adversaries across all the domains – land, sea, air, space and cyber. The government has been an early adopter of 5G technology, and we will continue innovating to support their unique missions. It's going to take more than mobility for the DOD to maintain domain superiority; the DOD will need all-encompassing solutions with defense-in-depth capabilities, built upon a foundation of cybersecurity.

"It's going to take more than mobility for the DOD to maintain domain superiority; the DOD will need all-encompassing solutions with defense-in-depth capabilities, built upon a foundation of cybersecurity."

- John M. Dillard

B Government Business Council

About GBC

As GovExec's research division, Government Business Council (GBC) is dedicated to advancing the business of government through analysis, insight, and analytical independence. An extension of Government Executive's 50 years of exemplary editorial standards and commitment to the highest ethical values, GBC studies influential decision makers from across government to produce intelligence-based research analysis.

Learn More

AT&T

About AT&T

Our first name has always been American, but today you know us as AT&T. By bringing together solutions that help protect, serve, and connect—committed AT&T professionals are working with the public sector to transform the business of government. No company is more invested in America's future than AT&T.

Learn More