verizon | Pixel for Business

Embracing 5G

Leveraging next-gen mobility and AI for federal agencies

Across the defense and civilian landscape, agencies seeking battlefield superiority and increased citizen engagement are eager to embrace mobility and leverage the power of 5G networking.This includes equipping personnel with advanced mobile devices capable of harnessing the full potential of 5G.

5G's low latency, mobility and high speeds can bring new capabilities to life for military organizations, at a time when potential near-peer conflict intensifies the value of reliable communications. In the near future, "they're going to be using wireless just about for everything," said Jodi Renbaum, Verizon's business development client partner for DOD Mission Critical Networks. This shift necessitates robust, secure and versatile mobile platforms.

During a recent ATARC roundtable hosted by Verizon and Google Pixel for Business, military leaders and industry experts took a deep dive into the topic. Participants included representatives from the U.S. Space Force, U.S. Naval Research Laboratory, U.S. Department of Defense (DOD), Defense Logistics Agency, U.S. Navy and the DOD Digital and Artificial Intelligence Office. It was discussed how agencies can adapt their networking and IT strategies to make the most of emerging opportunities like 5G and AI in a mobile world, including the use of mobile hardware for critical operations.

Unlocking AI's potential: The role of networking and mobility in military operations

Creating a security-first, digital transformation strategy that utilizes modern infrastructure, software-defined networking and cloud-based controls can make it easier for organizations of all sizes to deploy new applications and services, including artificial intelligence. This strategy should also consider the increasing importance of mobile devices in accessing and utilizing these services.

While there is a lot of press about large AI models providing a wide range of capabilities, the specific capabilities needed in any particular instance are likely to be more targeted. Support for mobile use cases, for example, requires the ability to scale the size and functionality of the AI model to suit the device's capabilities. The combination of Google Pixel devices and Verizon's network capabilities enables this as a seamless experience.

AI models that provide the ability to scale from large-scale services to edge computing (with no data leaving the device) will be critical to enable a wide range of use, including when edge devices go offline. The ability to seamlessly move from local to service-oriented models, all without the user needing to make a choice, will be critical. Advanced mobile hardware, combined with robust network infrastructure, is essential for enabling this seamless transition.

AI is poised to revolutionize various aspects of civilian and DOD operations. A modernized, intelligent network infrastructure with the right mobility tools, including powerful smartphones and other mobile devices, is crucial for harnessing AI's potential.

Implications for military operations

The integration of AI-powered networks and hardware is revolutionizing military operations, offering transformative benefits across key areas. From enhancing situational awareness and communication to improving efficiency and strengthening cybersecurity, AI can help empower forces to operate with greater precision, adaptability and security.

1. **Enhanced situational awareness:** AI-powered networks provide real-time data for informed decision-making. AI-powered hardware can enhance situational awareness, run specialized apps for first responders and support government-approved security apps for secure communication and data access.
2. **Improved communication:** AI-optimized networks enhance seamless communication between troops, commanders and allies. AI-powered translation tools on the actual device can help bridge communication gaps between US forces and local populations in foreign environments. This can facilitate cooperation, gather intelligence and reduce the risk of misunderstandings
3. **Increased efficiency:** AI-driven automation streamlines logistics, supply chain management and other operational processes.
4. **Cybersecurity:** AI-powered networks detect and respond to cyber threats in near real-time. On device threat detection, enhanced security features and privacy protection bolstered by AI protects agencies.

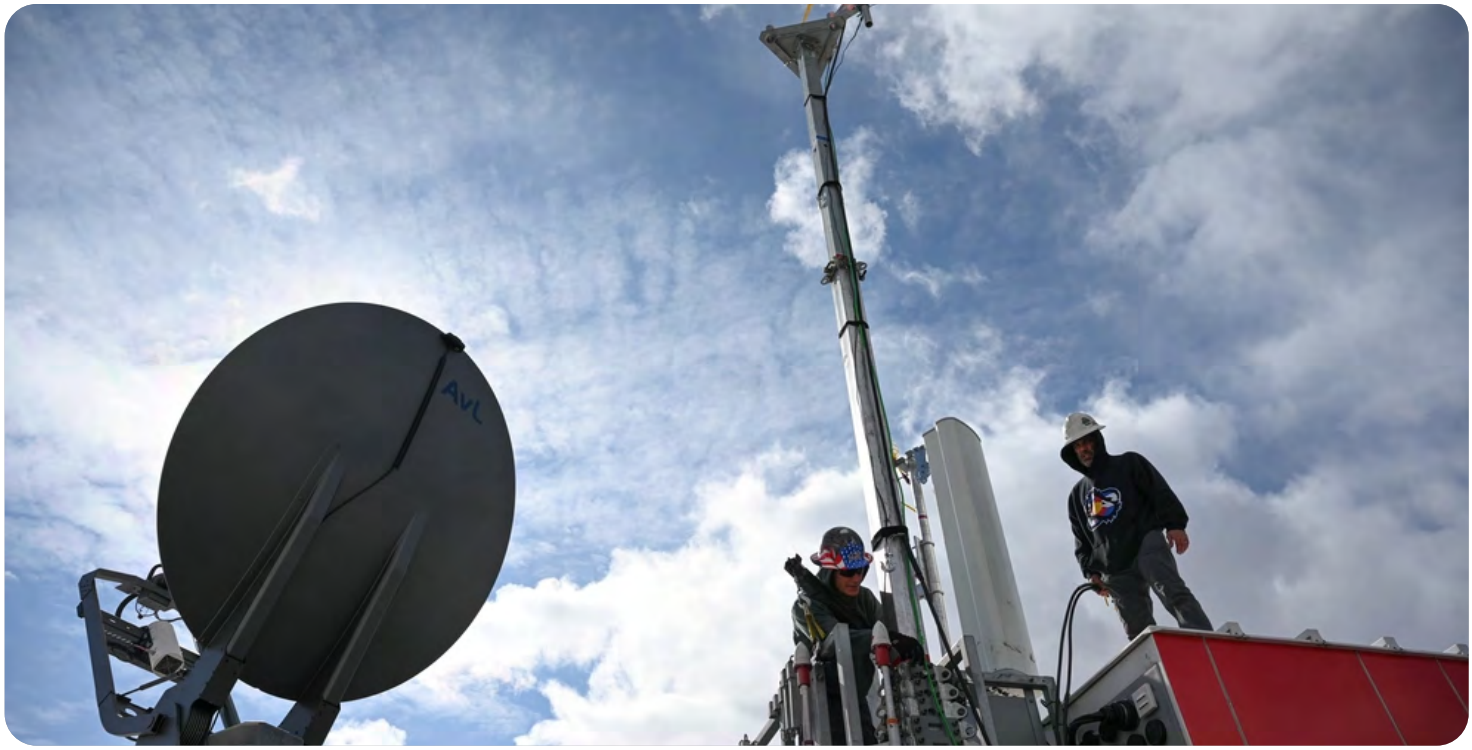
In the near future, "they're going to be using wireless just about for everything."

Jodi Renbaum, Business Development Client Partner, DOD Mission Critical Networks, Verizon

Hardware selection:

Selecting the right hardware is essential for maximizing the potential of AI in modern mobile devices. From enabling on-device processing and efficient AI models to seamless cloud integration and offline functionality, hardware innovations like those in Google Pixel devices demonstrate how cutting-edge technology can enhance AI performance, scalability and user experience.

1. **On-device processing:** AI can optimize on-device processing, which protects sensitive information, enables rapid decision-making, minimizes data transmission and ensures operation even in offline environments. Pixel, powered by its custom AI chip and Gemini Nano, exemplifies this by bringing powerful AI capabilities directly to the device.
2. **Efficient AI models:** Scalability and efficiency are paramount with AI. Google's AI architecture exemplifies this by intelligently distributing workloads. It leverages an ecosystem of AI models, from lightweight versions on the Pixel device to powerful cloud-based models for complex tasks.
3. **Seamless usage:** AI needs to seamlessly transition between the device and the cloud, providing access to larger models when needed without any user-perceived delay. Pixel was designed with AI at its center and can dynamically and seamlessly blend on-device and cloud processing.
4. **Improved CPU:** CPUs deliver better performance, and in some cases, dedicated AI processing for better edge computing support. Pixel's development based on AI design delivers that.
5. **Off-peak processing:** Smartphones can be programmed to perform less urgent AI tasks during off-peak hours. This is when network congestion is lower, allowing for more efficient use of resources. Pixel devices are able to utilize this capability.
6. **Offline features:** Offline functionality must be done at the edge, maintaining critical capabilities in any situation. Pixel's AI capabilities such as Live Translate, speech-to-text and basic image processing are able to work without an Internet connection addressing concerns around data privacy and latency.
7. **Federated learning:** Mobile devices can participate in federated learning, where it trains AI models locally and only shares small updates with the cloud, minimizing data transfer while contributing to a global model. Google has designed its own federated learning model.
8. **Security certifications:** It is crucial for a smartphone to meet multiple federal requirements and that what is chosen is secure. Google Pixel features numerous federal security certifications such as, DoDIN APL, NIAP, CSfC, DISA STIG. Learn more here.



Long-term solutions for both network and mobility:
To meet the growing demands of AI-driven systems, a comprehensive approach is essential, focusing on the integration of advanced infrastructure, optimized management and cutting-edge hardware. Key solutions include:

1. **Complete digital infrastructure:** A fully digital infrastructure to support seamless AI integration across all devices and platforms.
2. **Software-defined networking (SDN):** Centralized network management for improved flexibility and optimized data transfer rates from mobility and reduced latency.
3. **Network function virtualization (NFV):** Virtualized network functions for increased scalability and adaptable distributed architectures to handle evolving demands
4. **AI-optimized hardware:** Advanced hardware, such as dedicated AI processors and optimized memory architectures, will be crucial for enabling faster and more efficient processing for on-device AI tasks. This will empower devices to handle increasingly complex AI workloads without relying solely on cloud resources
5. **Enhanced security and efficiency:** Isolated network segments and prioritized data transmission alongside on-device data protection and secure processing environments to minimize bandwidth use and support complex AI workloads.

5G Private Networking: Low-latency, high-throughput AI applications rely on dedicated, secure wireless infrastructure. 5G private networks provide this foundation, enabling real-time edge processing and granular resource allocation for optimal AI system performance.

AI for defense mission success

By upgrading network infrastructure and adopting a complete digital framework alongside mobility hardware, military organizations can mitigate the challenges posed by AI's impact on network performance and unlock the full potential of AI applications.

AI is already transforming training and battlefield operations, providing near real-time insight into on-the-ground conditions so that commanders can make better decisions. Although this is a powerful example, the use cases for AI in defense could be far more expansive and profound than what we've seen so far.

Experts are already using AI to analyze satellite images and drone video feeds faster than before. This visual intelligence can be particularly valuable on the battlefield, helping military forces understand the current state of play. This can translate directly into the capability to react more quickly in critical fast-moving situations in the field. Mobile phones, with their chips and software optimized for AI processing, could be used to analyze this imagery directly on the device, even in offline environments. This edge computing capability could drastically reduce latency and provide real-time insights to soldiers in the field.

Federal civilian agencies are already seeing wins here that could help inform DOD's efforts. In some cases, AI-supported security solutions "continuously monitor the edge with tools that can detect nefarious threats and deny them access," said Rudolf Rojas, an information technology manager at the Department of Agriculture. The same approach could help secure warfighters' devices at the tactical edge.

Meanwhile, defense agencies seeking to deploy their own AI-driven applications in turn can look to the network to help drive those efforts. This requires a thoughtful look at the infrastructure and hardware selection.

Real-world applications
These advancements are driving improvements in communication, intelligence gathering and cybersecurity, enabling the Department of Defense to operate more effectively, securely and efficiently in mission-critical environments.

In some cases, AI-supported security solutions "continuously monitor the edge with tools that can detect nefarious threats and deny them access."

Rudolf Rojas, Information Technology Manager, Department of Agriculture

[1]Not available in all languages or countries. Not available on all media or apps. See g.co/pixel/livetranslate for more information. Translation may not be instantaneous.

“Everybody likes to talk OT, but we really don’t just have OT anymore. We have IT-automated systems. We should redefine everything. You put a computer on it? It’s IT.”

Shane Williams, Enterprise Information Systems Security Manager, Defense Logistics Agency

1. **Tactical networks:** AI-optimized networks for battlefield communications and hardware capabilities with integrated walkie-talkie functionality and long battery life help ensure uninterrupted communication and productivity.
2. **Intelligence, surveillance and reconnaissance (ISR):** AI-powered networks for real-time data analysis and AI powered hardware for evidence collection and open source intelligence.
3. **Cybersecurity operations:** AI-driven networks for threat detection and response. AI powered hardware built with multiple levels of hardware security and amplifies zero trust capabilities.

By integrating AI with modern network infrastructure and mobility, the DOD can unlock new possibilities for efficient, effective and secure military operations.

Build a roadmap to modernization

AI can significantly impact network performance due to the large amount of data required for processing and analysis. Key factors include data volume, bandwidth requirements, latency and network congestion. Some military organizations may still need to look at their network infrastructure to make sure they have the network and right set of mobility tools to support the data gathering capabilities that AI applications need before they can embrace AI technology. Mobile devices, with their advanced on-device processing capabilities such as Pixel can help reduce the reliance on constant network connectivity. By performing initial data processing and analysis on the device itself, they can minimize the strain on the network and improve overall efficiency.

IT needs to understand how much data existing infrastructure can support with AI integration. Generative AI, for example, can add increased data needs to the device data load, and in order to support that need, IT needs to upgrade the existing networks’ capacity and performance. New emerging technologies including mobility hardware and private 5G networks can provide high performance communications security, privacy, higher bandwidth, performance and low latency with QOS required for complex operations and algorithms. There’s a road to modernization that needs to be traveled first before you see the full proliferation of AI across an office setting or a military installation, and transport mediums like 5G are going to be critical to those types of capabilities.

As DOD organizations look to modernize their infrastructure with an eye toward AI applications, “you have to define all the different silos of the network from layer one to layer seven, and what fits in those silos, and how each silo will be impacted based on what action you’re going to take for each,” Rojas said.

To build an AI-capable networking solution, it’s important to start with a roadmap that lays out the long-term vision. “Then you continue to work on that vision,” he said. “It may take three years, it may take five years...but you have to really start, and do the due diligence.”

Treat OT like IT

In the past, Information Technology and Operational Technology have lived in separate siloes. It’s becoming increasingly important to view them through a single lens. “The lines between OT and IT have become so blurred,” said Shane Williams, enterprise information systems security manager at the Defense Logistics Agency (DLA).

At DLA, that blurring has been deliberate: “We started punching holes through the wall,” Williams said. It’s been necessary to do that, as functionality increasingly overlaps in the IT and OT realms. “Everybody likes to talk OT, but we really don’t just have OT anymore. We have IT-automated systems.”

“Defining your business needs will help develop the scope and priorities that will help set clear goals and objectives and make sure that all the parties that you’re going to work with, including your vendors, have a strong buy-in.”

Mohammad Rehman, Solutions Architect, Verizon

In the current environment, “I’ve got IT systems that are monitoring OT systems,” he said. That being the case, “we should redefine everything. You put a computer on it? It’s IT. I don’t care if it’s the HVAC system, if it’s the electrical system.”

The mobile ecosystem plays a key role in supporting OT applications on military installations and elsewhere in the DOD.

Here, a modernized approach helps to make possible the integration of IT capabilities. Built-in security mechanisms, such as protected APIs, make it possible to bridge the IT and OT environments “without getting crazy and over-architecting solutions,” said Mike Burr, Google’s senior security consultant for Android Enterprise.

In order to get IT and OT together in a single view, Mohammad Rehman, Verizon solutions architect, said some culture-change will be required. “One of the challenges even for CIOs is: How can I bring all these parties together within their internal organization?” he said. This will help with the integration of infrastructure innovation and modernization.

To move the needle, IT leaders across the defense landscape will need support from the vendor community. They should be “working with the partners and understanding what they have to offer,” he said. This will help to ensure that all are aligned around the effort, and driving toward the same end result.

“Maybe there are opportunities that I didn’t anticipate,” he said. There may be a place to bring mobility to the fore even though that use case “wasn’t necessarily on the radar.”

George Chambers, Acting CIO, Department of Health and Human Services

AI’s impact on network performance and on mobility:

AI applications can significantly strain both network performance and mobile devices due to the large amounts of data required for processing and analysis. Key factors affecting performance include:

1	**Data volume**	Large amounts of data generated by AI applications.
2	**Bandwidth requirements**	High-speed data transfer rates required for AI processing.
3	**Latency**	Delay in data transmission and processing.
4	**Network congestion**	Overwhelming network traffic.

To address these challenges, military organizations can consider the following strategies:

Network infrastructure upgrades:

1. **Fiber backbone:** High-speed fiber-optic connections for reduced latency.
2. **TDM over IP:** Legacy system support for seamless integration.
3. **Distributed architecture:** Decentralized architecture for improved scalability.
4. **Edge processing:** Data processing at the edge of the network for reduced latency.
5. **Network segmentation:** Isolation of critical network segments for enhanced security.
6. **Quality of service (QoS):** Data prioritization for optimized network performance.
7. **Satellite connectivity:** Addressing coverage gaps in remote areas through satellite connectivity to expand network reach and ensure consistent service.
8. **5G network slicing:** Utilizing 5G network slicing enables dedicated virtual networks with tailored QoS that could prioritize AI traffic with specific bandwidth and latency requirements.

Focus on proof of concept

With any effort to modernize the infrastructure, it's important for defense agencies to start with a proof of concept. And that effort needs to be well thought out.

"Defining your business needs will help develop the scope and priorities that will help set clear goals and objectives and make sure that all the parties that you're going to work with, including your vendors, have a strong buy-in." Rehman said

As Acting CIO at the U.S. Department of Health and Human Services, George Chambers said the proof of concept can also be a means to uncover unforeseen opportunities for mobility. "Maybe there are opportunities that I didn't anticipate," he said. There may be a place to bring mobility to the fore even though that use case "wasn't necessarily on the radar."

In defense agencies, too, a well-defined proof of concept should be flexible enough to recognize and adapt to the unexpected.
Some proof-of-concept efforts take years, while others come to fruition in just weeks, depending on the complexity of the mission. The collaborative effort may involve government labs, universities and partners like Verizon, Google and system integration partners. "We come together in the lab and define the clear objectives, realistic scope, complexity, measurable success criteria, testing, refining and project deliverables," Rehman said.

Take a hard look at security

Technology is an adversarial space in modern warfighting. That means security considerations must be front and center, as the IT infrastructure evolves. Yet too often, "the vendor comes along and slaps security on after the fact," Williams said. The DOD needs a more robust approach.

The DevSecOps approach helps to mitigate this tendency, and an IT overhaul would go even further. Defense agencies "need to get rid of all these legacy systems that are sitting out there" that rely on bolted-on security solutions, he said.

Renbaum pointed to Verizon's innovation labs in Ashburn, San Francisco and Boston as well as Google's innovation labs in California, Washington, D.C. and New York as key support here, and Rehman described the importance of incorporating zero trust. While zero trust enhances security, it's crucial to ensure it doesn't compromise usability.
By striking a balance between security and usability, organizations can effectively implement zero trust with minimal compromising of user experience.

With zero trust, "you're overlaying different protocols on security, plus encryption, [and] that really puts a lot of load on a device and then the network," he said. For warfighters and military decision-makers who need to utilize mission-critical applications, it's important to ensure device and application access still is "seamless to the user."

As mobility and the Internet of Things (IoT) emerge as essential battlefield enablers, Android has staked out a place as an industry leader in overall security, Burr said.

"We're seeing a lot of these older IoT devices being replaced with devices that have Android on them [because] the Android operating system itself is highly secure," he said.

"People are really paying attention: They're starting to replace these old infrastructure components at the edge where there are remote capabilities, or you need to prevent hacking."

Mike Burr, Senior Security Consultant, Android Enterprise, Google

“At Google, not only do we develop the hardware, we also develop the platform, anything from the silicon back to the solutions. We like to say that we can bring end-to-end solutions to the government.”

Sharmeen Noor, Federal Partnerships and Solutions Lead, Google Pixel for Business

“People are really paying attention: They’re starting to replace these old infrastructure components at the edge where there are remote capabilities, or you need to prevent hacking.”

AI has a key role to play here. As defense agencies look to protect their systems against adversarial intrusion, AI can help to “prevent and mitigate” cyber events, for example by automatically blocking phishing attempts. That is important, he said, since “users will always be users. No matter how compliant you try to make them, they will always do what they want to do.”

To Burr, devices should also be evaluated based on their security certifications and the devices are “Secure by ” meaning that security is incorporated into every part of a device’s creation, from the initial concept to its ongoing maintenance.

Key takeaways

A security-first, digital transformation strategy is essential for leveraging AI’s potential across modern infrastructure and mobile devices. By combining advanced mobile hardware with intelligent network capabilities, organizations can achieve significant benefits:

1. **Optimized network performance:** AI maximizes throughput, reduces packet loss and minimizes latency. AI, through its devices, can intelligently prioritize network traffic and perform near real-time analysis of network conditions.
2. **Automation and predictive analytics:** By leveraging automation and predictive analytics, AI strengthens network resilience. An AI-powered system can analyze network traffic in near real-time, detecting security risks and potential failures. This analysis drives automated troubleshooting and enables self-optimizing networks, where AI dynamically adjusts configurations based on performance data, identified issues, and proposed solutions.
3. **Open systems interconnection (OSI) framework:** AI supports modern network connectivity within the OSI framework. AI through devices can optimize communication protocols across different layers of the OSI framework.
4. **Adaptive security:** AI strengthens device and network security by proactively identifying and mitigating threats in near real-time
5. **Processing power:** AI on mobile devices can help reduce latency and dependency on cloud connectivity. AI models scaled for mobile devices can prevent excessive battery drain or performance degradation. This scalability allows for a wider range of AI applications on mobile devices.

Build a team of partners

In order to move forward effectively, military IT leaders should look to build a capable team of partners. They need a wide range of capabilities in order to “deliver something that is end-to-end, that is obviously cost efficient, and also works seamlessly and automatically together,” said Sharmeen Noor, who leads federal partnerships and solutions at Google Pixel for Business.

Although agencies “tend to operate in silos,” even within the DOD, many are coming to recognize the value of a broad-based approach to modernization, she said, noting that it takes a mix of capabilities “to be able to solve a lot of those pain points.”

“At Google, not only do we develop the hardware, we also develop the platform, anything from the silicon back to the solutions. We like to say that we can bring end-to-end solutions to the government,” she said. Google Pixel in particular offers a way to bring that broad-based vision to life, serving as “the entry point to the rest of the Google ecosystem.”

As military agencies look to expand their mobile capabilities, a partner ecosystem can help to drive success. Together, Verizon, Google and partners “can integrate this with the legacy systems,” Rehman said. With a combination of intelligent networking including private 5G, security cloud and mobile edge computing capabilities, “with the goal to reduce latency, for good user experience.”

Learn more about how Verizon and Google Pixel are harnessing mobility and AI to help transform federal operations.