Terry White

JOHNNY SHRYOCK PHOTOGRAPHY

THE NETWORK OF TOMORROW, TODAY

Modernization can help the National Guard meet the mission.

By Adam Stone

The National Guard needs robust connectivity to support every aspect of its warfighting mission abroad and its vital humanitarian work at home. The network is the backbone of the modern military mission, from soldiers in the field, to manned and unmanned aircraft, to data-rich communications and emerging Internet of Things deployments.

Networking demands are changing the very nature of the National Guard mission. In day-to-day operations or preparing for and during times of crisis—connectivity is critical. Secure communications must reach the soldier, especially in damaged or remote areas during an emergency.

LEGACY CHALLENGES

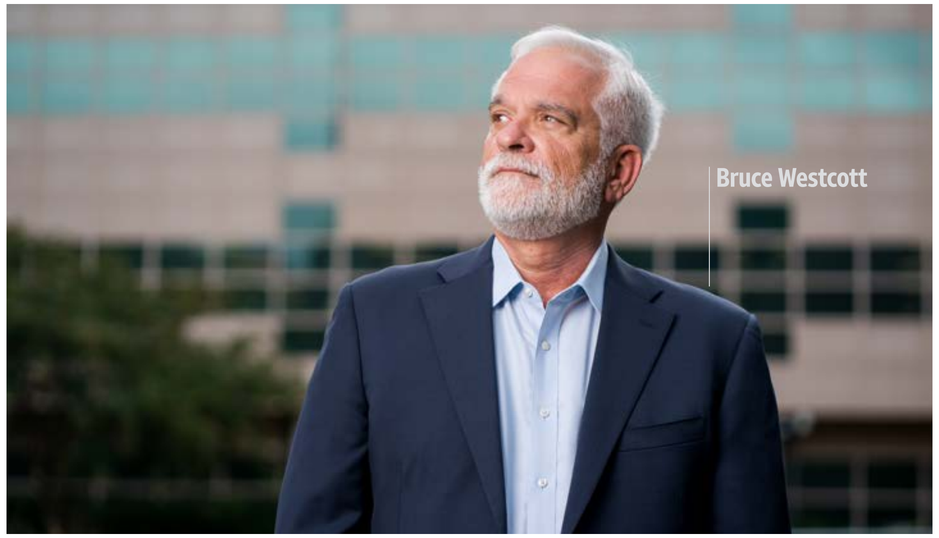
Several factors come together to limit the utility and cost-effectiveness of the National Guard's legacy telecommunications network infrastructure.

Consider for example the proliferation of communications devices at the tactical edge. "In a world where everything is mobile, these legacy systems were not designed for handheld devices or laptop devices. They were not designed to support technology inside of vehicles that are moving from place to place. That presents challenges for the Guard," said Terry White, Director, Client Executive for Army and National Guard at AT&T Public Sector.

Legacy systems are also costly to maintain: Nearly 80 percent of the government technology spend goes to the care and feeding of such systems. "If the Guard can find a way to modernize, to migrate from these systems that are using old codes and old infrastructure, it would be much more cost effective," White said.

At the same time, commercial networking capabilities are expanding at a rapid pace, and the older systems often cannot keep up with these new innovations. That makes it harder for the Guard to meet its mission objectives, with bandwidth limitations and other constraints hindering effective communications.

"It's important, to look at it from the soldier or the airman's perspective," said Bruce Westcott, Director, Strategy and Solutions, for Army at AT&T Public Sector. "They may have more capabilities on their home devices than they do when they leave for drills or training. At home, they're streaming video, they're gaming or doing online activities. When they're in the armory, they're using a TDM T1 line that's at least 15 years old. In the commercial world, technicians are no longer trained to fix TDM networks, so the Guard faces challenges with aging equipment when fewer resources are available."



EMERGING LANDSCAPE

In the commercial world, networking is quickly evolving beyond the old-school model of routers and switches upon which the Guard still relies. Modernized networking looks beyond hardware, tapping the power and flexibility of software to drive enhanced connectivity.

"Just five or seven years ago, there was a box, a router or a switch that performed a function," White said. "The industry is moving towards leveraging software that will perform these different capabilities or functions. This would allow the Guard to be able to stand up and move swiftly. The Guard is a rapid response organization, and we want them to have a network that allows them to be exactly that."

Modernization also promises to enhance security. Network security today is a labor-intensive manual task, requiring administrators to download and implement a seemingly never-ending series of patches and upgrades.

"That approach to security is antiquated, it's costly, and it puts a degree of risk into the National Guard network," Westcott said. "By moving toward software-based infrastructure, we, as the service provider, can manage and protect their network remotely, digitally and quickly."

With AT&T managed network security, the Guard could modernize network security without cost-prohibitive capital investments. The ability to forecast monthly expenses would make it easier to meet budget, often at significantly lower cost than managing security in-house.

THE "AS-A-SERVICE" MODEL

When networking infrastructure is built on software, connectivity and capabilities can be delivered "as a service." In this model, the end user has ready access to communications tools at scale, with the ability to leverage what's needed at a moment's notice. This aligns closely with the scope and pace of the National Guard mission.

In a legacy network, Guardsmen may not have ready access to the bandwidth needed to support robust communications—for example, the ability to send and receive video in a crisis when many end users are actively using the network. "When they migrate to networking as a service, that capacity is consistently available," White said.

The as-a-service model updates the Guard's acquisition strategy. Rather than continue with a build/operate/defend position, the Guard could leverage the as-a-service model to deploy a network that is software-defined, orchestrated and cloud-enabled. This infrastructure would also leverage commercial carrier-grade security and include wireless technologies that embrace the Internet of Things. As-a-service networks can be deployed in minutes rather than weeks, and it can support highly secure VPN communications that never touch the public internet.

In this model, the Guard is free from having to devote resources to systems upkeep. Maintenance and upgrades happen automatically. "As a commercial service provider, we already keep pace with the latest capabilities and the fast-moving technology innovations. By allowing the service provider to deploy and manage the network, the Guard will have an infrastructure that will be intrinsically more up to date," White said.

SOFTWARE-DEFINED NETWORKING

Another hallmark of the modernized network, the term "software-defined networking" (SDN) describes an architectural approach in which the network is intelligently and centrally controlled using software applications. SDN delivers a high level of flexibility by decoupling the network's control and data-forwarding planes, by providing a centralized, cloud-based approach to network control.

In support of the National Guard's mission-critical tasks, one of the most important jobs of the network operator is to maintain a high level of network service quality. SDN makes it possible to quickly resolve issues by leveraging automation, advanced analytics and machine learning to enable more intelligent decision making.

Frost & Sullivan identifies AT&T as "among the few providers that have launched SDN-based network services to offer dynamic bandwidth services," making it one of the foremost leaders in the space.

With SDN, software could for example define a firewall, or it could route data and traffic, based on algorithms and predefined rules. Compared to an equipment-based architecture, this approach offers greater agility and flexibility. SDN drives significantly improved network response times, which can be critical as the Guard engages in its life-saving missions.

"Traditionally, if you're at the armory and all of a sudden you can't communicate or send emails, then you have to pick up the phone—hopefully it works—and call someone to say you have a problem," Westcott said. "With SDN, the network uses self-healing architectures and restoration technologies to maintain reliability. It's instantaneous, with no human intervention."

MODERNIZATION SUPPORTS CYBERSECURITY

By leveraging networking as a service, supported by a software-defined approach to network architecture, the National Guard could see significant gains on the cybersecurity front. Modernization delivers a highly secure network, with less manual intervention.

As with other governmental entities, the National Guard today faces threats from abroad, and the network is often viewed by bad actors as the target of opportunity.

"The conventional fix involves equipment, manpower and a lot of resources," Westcott said. "A better approach is to harden your network—to stop these bad actors from penetrating your network in the first place. In a modernized network, you shut down all the attackers and allow only the good traffic to pass."

The Guard could do this more effectively by working in close consort with a major service provider. AT&T is in a unique position as a network provider, with more than 350 petabytes of network traffic traversing our network in 200 countries and territories every day. "We use those insights to help protect our clients' networks, looking for indicators of bad data or threats to our customers," White said.

"The firewall is pretty much the outer gateway to any enterprise, but before anything gets to your firewall, it travels across our network. A service provider like AT&T can analyze data traversing the network, which gives the Guard another layer of protection," he said. "We have solid measures in place to ensure that our network is highly secure, which means we can simplify the number of security products that a customer may have to monitor and update."

MOVING TOWARD 5G

Network modernization also makes available all the robust communications capabilities inherent in the emerging 5G network technologies.

5G with related Edge technologies offer low latency—the gap that occurs as data travels across the network. Low latency could support an enhanced user experience in virtual training, with AI-enabled simulators making it possible for the National Guard to deliver immersive training in remote settings. This could eventually represent a major savings in terms of time and travel expense. It could also help ensure that Guardsmen across the country have a common training experience.

5G is also capable of supporting the growing Internet of Things. "The Guard needs to know: Where are their containers, where's the water, where are the trucks? With 5G and edge computing, the Guard can process massive data sets of this information locally and in near-real time, which is critical to mission success," White said.

"You'll eventually be able to connect massive numbers of devices and bring multiple sets of individuals together using 5G. And with edge computing, you'll be able to collect and process data from all these devices, as well as talk to your battalion commander, brigade commander, and staffs—all in near-real time," Westcott said. "5G enables faster and more effective collaboration."

With robust security, software-defined networking and future 5G connectivity assured, a modernized network delivered as a service could help the National Guard to meet the challenges of today and position itself for future success.

FirstNet and the National Guard

AT&T WAS SELECTED by the First Responder Network Authority to build and manage FirstNet, the only nationwide, high-speed, broadband network designed specifically for public safety. It is the first of its kind: the only wireless communications platform that has been architected from the ground up specifically to meet the needs of the nation's first responders.

FirstNet offers the National Guard a means to communicate through any crisis, with bandwidth sufficient to support video sharing, as well as prioritization and preemption to help ensure first responders always have ready access to communications.

As the only carrier with access to Band 14, AT&T is uniquely positioned to help the National Guard leverage the power of this emerging network. While others may claim to offer first responders a degree of priority and preemption, only AT&T has built an entirely separate network that can be dedicated to supporting those needs.

As 5G rolls outs nationwide, FirstNet will incorporate that next-gen speed, scale and low latency performance. And FirstNet is designed with modernization top of mind: AT&T has a 25-year contract with the federal government to manage and advance the infrastructure. "We've already completed more than 80% of the planned FirstNet Band 14 rural & non-rural square mile build ahead of schedule, in 700+ markets across the country, including rural towns and every major city coast to coast." said Bruce Westcott, Director, Strategy and Solutions for Army at AT&T Public Sector.

AT&T

Continue the conversation at
att.com/publicsector