TOUGH networks for TOUGH missions

BY JOHN EDWARDS

Navy Seals, Army Rangers, Air Commandos, and other special operations forces (SOF) rely on network hardware and services to access fresh, accurate intelligence and situational awareness information, often under severe pressure in extreme situations and environments.

Yet, unlike most deployed forces, SOF units rarely have the luxury of taking a full complement of network data equipment on their missions. "SOF deploy and operate in small teams, which require small communications packages capable of providing high bandwidth access to secure and nonsecure data, voice and video services to a small team anywhere in the world," said Bill Burnham, technical director of the U.S. Special Operations Command (SOCOM) J6, based at MacDill Air Force Base in Tampa, Fla. "Full communications services ... are rarely provided at the small team level," he added.

FAST AND NIMBLE

"Small and scalable is crucial," said Jerry Mamrol, director of land forces/C4ISR, for Lockheed Martin Information Systems and Global Solutions in Bethesda, Md. "Agile, persistent and flexible size is a focus because we're typically talking about special teams that don't have the kind of support and infrastructure that the broader Army would have."

Despite size, weight and power (SWaP) challenges, SOF still have access to a wide range of sophisticated network devices, thanks to ever-shrinking form factors. "SOF teams deploy with normal networking IT equipment ... such as laptops, printers, small communication servers and small satellite radios used to connect back to the SOF Information Environment (SIE) over the horizon," Burnham said.

SOCOM has special, service-like acquisition authorities, which allows it to access equipment to satisfy SOF-unique requirements. "To execute the acquisition mission for SOF, SOCOM has a Special Operations Research Development and Acquisition Center (SORDAC) with program executive offices responsible for the different mission areas, each with programs of record charged/funded to satisfy specific approved SOF requirements," Burham said. "Inside SORDAC, also, is the science and technology (S&T) division, which focuses on cutting-edge technology that could be used to satisfy a difficult SOF requirement, if invested in during early stages of development."

To maintain full interoperability and reliable connectivity, SOF teams typically deploy with standards-based networking and IT equipment. "Ethernet is still the predominant means of connectivity for systems at a SOF team location, via Wi-Fi, and Windows is the predominant operating system," Burnham said. "Most SOF development in the networking/IT arena focuses on improving the SWaP of the equipment, so that it is smaller, lighter and uses less power," he added.

New networking approaches also help SOF stay agile, flexible and secure. "From head-of-state missions to tactically deployed forces, the traditional thinking was to deploy the entire network to support the mission," said Chris Herndon, vice president and chief technology officer of the national security group at SRA International, an information technology services and solutions consulting company headquartered in Fairfax, Va. "Satcom technologies have become smaller, better modulation techniques and robust crypto supports rapid deployment of private networks virtually anywhere in the world." Herndon added that "the real paradigm shift ... is the movement to the commercial networks—not just the U.S. networks, but host nation infrastructure worldwide."

Emerging technology now allows SOF to operate flexibly and securely almost anywhere on private networks. "The technology

LUIS VALDESPINO JR./DEPARTMENT OF DEFENSE

Special operations forces teams rarely deploy with full communications services. They rely on small communications packages capable of providing high bandwidth access to secure and nonservice services anywhere on the globe.

evolution we are seeing now allows devices to interoperate on multitude of host nation networks while still providing an acceptable level of security and protection without the cost or manpower of deploying private networks," Herndon said. "Add to that the sophistication of being able to obfuscate the transactional data from these devices and we have the capability of hiding in plain sight on someone else's network."

SOCOM also strives to maintain full interoperability with other forces. "SOF acquires radios that are compatible with JTRS waveforms to ensure compatibility on the battlefield with service forces," Burnham said. "SOF relies on support from non-SOF organizations during operations, so must remain able to communicate via service/joint common communications systems."

SOCOM must also evolve SOF communications capabilities in synchronization with other forces. "Going forward with the mobile user objective system (MUOUS) in place now, that will be a waveform that [SOF] will be able to take advantage of," Mamrol said.

TURNING TO COTS

SOCOM, like services and units across the military, is increasingly turning to commercial-off-the-shelf (COTS) devices to take advantage of their generally lower costs, native interoperability, innovative features and reduced R&D requirements. "They can't afford to keep recreating or having unique one-offs," Mamrol said. "Maybe that was tolerated before because of the priority of the mission, but as we draw down and budgets grow tighter I think interoperability and standardization is going to become more and more important."

Yet Burnham noted that deploying COTS devices also poses a challenge. "Commercial/consumer grade IT equipment often falls short of the DoD's cybersecurity, ruggedness and SWaP requirements, and the business case for building COTS equipment to DoD standards is difficult for commercial vendors to make when DoD requirements may be in the thousands [of units] while consumer demands are in the millions," Burnham said.

Device ruggedness is a particularly important concern for SOF. SORDAC program managers, however, aren't reluctant to harden COTS equipment for SOF use. "This happens frequently with COTS networking equipment, like routers and switches, which are repackaged [by SORDAC] in rugged cases with shock absorbing mechanisms and air filtering capability," Burnham said.

Security is another top priority for SORDAC program managers. According to Burnham, most COTS mobile devices, such as smartphones and tablets, fail to meet DoD security requirements. "SOCOM's current mobile device efforts focus on ... BlackBerry 10 mobile phones, which securely connect back to the BlackBerry Enterprise Server in the SOF enterprise, and Windows tablets connecting via Wi-Fi, both of which have been approved for use on DoD networks," Burnham said.

SOCOM's unique acquisition authorities are critical to meeting operation demands. "Recent budget issues have slowed some acquisition efforts, but no high-priority technology programs have had to be terminated," Burnham said.

He added that fiscal 2014 priorities remain to equip SOF operators as a system and ensure they have the communications infrastructure and equipment necessary to sustain operations. "In that regard, SOCOM is focusing on strategic, long-term technology that improves the protection and survivability of our deployed operators," Burnham said. "This includes interoperable technology that augments the real-time data requirements and improves situational awareness."

FUTURE PLANS

Burnham said SOCOM is always looking for ways to enhance SOF network technologies and capabilities. "Any improvements to SWaP are always of interest for SOF IT equipment, including improved battery performance," he said. "Additionally, improved video coders/decoders capable of further compressing HD video streams would be of interest, as would data encryption solutions that employ two layers of Suite B software encryption in accordance with the [National Information Assurance Partnership] protection profiles."

SOCOM also pays close attention to emerging network technologies that have the potential to benefit SOF. "Just as in the commercial world, the Internet of Things is on the horizon, and SOF will benefit by being able to securely connect people and equipment, which will increase our operators' situational awareness and speed their decision-making," Burnham said.□