The Voice of Military Communications and Computing

Military Information Technology

C4I Modernizer

Rear Admiral Patrick H. Brady

Commander Space and Naval Warfare Systems Command

www.MIT-kmi.com

MIT

C4

December 2010

Volume 14, Issue 11

Cyber-Ranges ✯ 3G/4G ✯ Army NETCOM ✯ Rugged Computers
Network Intrusions

Peering Into the 3G/4G Future

Adapting smartphone technology to the battlespace could allow for the exchange between the front lines and headquarters of text, data, pictures and video.

By Peter Buxbaum
MIT Correspondent
buxbaump@kmimediagroup.com

Imagine if frontline troops whipped out smartphones when they needed to communicate with each other or with commanders. The scenario is not so far-fetched. U.S. warfighters in Afghanistan and Iraq often carry cell phones on their persons. The military authorizes them to purchase subscriptions from local telecommunications providers and to use the phones on base as a morale booster. When out on missions, they will make use of those cell phones when all else fails.

Captain Joshua Dixon

"We used the cell phones as a tertiary communications device," said Marine Corps Captain Joshua Dixon, who recently received a master's degree in computer science and is currently working toward an MBA at the Naval Postgraduate School, referring to times when he was deployed to Southwest Asia. "If everything else went wrong, we would turn on the cell phones and get communications as a last resort."

Warfighters like Dixon grew up with mobile technologies available to them. Having used cell phones in theater as well, he recognizes the benefits they could provide U.S. troops. With third generation (3G) and coming fourth generation (4G) wireless technologies, adapting smartphone technology to the battlespace could allow for the exchange between the front lines and headquarters of text, data, pictures and even video, all in an effort to locate targets and achieve better situational awareness.

"During tactical operations, it was easy to recognize a number of gaps that these capabilities could fill," said Dixon. "Pulling and pushing information is easier if it is done through data. It is much easier to describe a local environment with pictures than through voice communications."

To be sure, introducing a new technology to a theater of operation is no simple matter. Neither the phones nor the commercial networks that connect them are up to military security standards. There are a number of issues that need to be worked out before cell phones and smartphones routinely connect warfighters in the battlespace.

3G and 4G smartphones have much greater capabilities than the field radios now carried by company-level ground troops, according to Dixon. "Currently radios are voice communication devices with the ability to transmit some kilobits of data, and that is not really used much at the tactical edge," he said. "Units at the battalion level and higher and some special operations units have some more advanced devices. But we are focused on the 95 percent of operations carried out by foot soldiers and mobile troops."

So Dixon embarked on a research project at the Naval Postgraduate School to see if cell phone technology could be adapted for military mission purposes. One aspect of his research was to

uncover any earlier programs that had tried to introduce cellular technology to the battlespace. One Army program started earlier in the decade failed "because they were trying to bring in a lot of capabilities and had to start prioritizing," said Dixon. "The cellular capability was too risky to bring in at that time."

The Joint Tactical Radio System program office had a cellular waveform in its portfolio, but dropped it after the office consolidated its wide range of programs. When Dixon began his research in 2008, there were no active programs of record among any of the armed services focused on the introduction of cellular technology.

"Our primary goal is to increase communication capabilities, while minimizing the amount, physical size and cost of the specialized hardware," said Dixon. "Cell phones possess the most desirable characteristics: low cost, small form factor, millions of daily users, hundreds of competing companies to develop the latest and greatest technology, and an abundance of other highly valuable features."

Jake MacLeod

Data Transmission Rates

The telecommunications evolution from 3G to 4G allows far more data to be pushed through to users much faster. In fact, data transmission rates for 4G are expected to go 50 times that of 3G. For Dixon, it makes sense for the U.S. military to investigate the adoption of these technologies.

"The easiest way to describe the difference between 3G and 4G is to analogize between dial-up Internet connections and DSL or cable," said Mike Ligas, director of DoD sales at Sprint. "All of a sudden you could transmit PowerPoint and spreadsheet files without waiting for them to upload. 4G also represents a quantum leap in the size of data files than can be transferred quickly."

Andrew Silberstein

"I think there is a huge opportunity for 4G in the military world," said Jake MacLeod, an executive vice president in the government solutions business of Powerwave Technologies, a supplier of antennas, base stations and other components for wireless networks. "4G opens up possibilities for the warfighter in the field to be able to able to use true broadband communications."

Roger Quayle

4G also brings a purely IP packet switched network to the communications picture, noted Andrew Silberstein, vice president and general manager at Globecomm Systems. "This beings a new level of efficiency to the use of bandwidth and spectrum," he said, noting that those two commodities are often in scarce supply on the battlefield.

Current warfighter mobile applications are hobbled by limitations on spectrum and backhaul, MacLeod explained. Backhaul refers to the capability to transmit data from the network edge to the network core, which is difficult in a mobile environment but is facilitated by 4G's fat pipe.

Increasing the 3G data rate from two megabits per second (Mbps) to 100 for 4G allows for a much larger pipe to provide additional information to the warfighter. "Right now, wireless networks primarily carry voice," said MacLeod, "but in the very near future, machine-to-machine communications will take up most of that pipe. Assets talking to each other will improve location awareness. This is going to have a huge positive impact on the warfighter."

The kinds of military applications that could be designed for 4G communications are limited only by the human imagination, according to MacLeod. "One application would be the locations of personnel and assets," he said. "If you are looking for a specific individual in a chaotic environment, you would be able to find him. By equipping personnel with a few small sensors, you could keep tabs on their vital signs and be able to determine their physical condition. You could identify friends and foes by the acoustic signatures of their weapons. You could design applications that could help with IED protection. By letting your mind run wild, you could come up with a tremendous number of secure applications that don't exist today given the wireless infrastructure available to the warfighter. That is what 4G brings to the table."

Sprint has packaged a number of 4G solutions of potential use to the military, said Ligas, including everything from base surveillance applications to setting up a mobile command center that includes a wireless hot spot for five to six users. Ligas envisions future applications to include the transmission of intelligence pictures to a helmet display of tank or ground force commanders, blue force tracking and providing situational awareness to all warfighters.

"I always think about what I would have wanted when I was in the Navy," said Ligas. "With 4G, commanders can have the ability to know what is happening all around them."

Commercial Infrastructures

One of the key issues to be resolved by the military as it considers adapting cellular technologies to the battlespace is whether it will insist on deploying private networks or whether it will agree to use existing commercial infrastructures. "Using commercial networks allows for greater availability of spectrum, but they are not as secure as the military would like, especially for classified traffic," said MacLeod. "Private networks are more expensive to deploy, upgrade and maintain. In the case of a commercial network is it is the carrier that does all of those things."

Silberstein has seen contract requirements for both kinds of arrangements. "The determining factor has to do with the specific applications that are involved," he explained. "In one scenario, the government might be looking to promote or advance a particular technology in a specific country. But there are applications where the government will insist on a closed network, and that typically includes a level of security and encryption. We are providing such closed systems to the Army where it does not want to interact with cell providers in a particular country."

IPWireless, a developer of 3G and 4G wireless solutions, addresses the military's needs to have a transportable communications solution in theater with what it calls a "network in a box."

"One box contains the core network and several small boxes contain the base station and radios," said Roger Quayle, the company's chief technology officer. "It can all fit in the back of a Humvee or on a helicopter."

The local private network created with this equipment comes not only to secure communications but to make them more reliable. "There are cellular networks operating in Iraq and Afghanistan, but their service is intermittent and unpredictable," said Quayle. "These are not technologies the military can rely on."

IPWireless has been involved in several trials and experiments to prove the viability of using 3G/4G as a last tactical mile technology for the military. The company's technology focuses on broadband data rather than voice. "We're not out to replace existing voice radios," said Quayle, "but to provide an additional capability." Users would access the network over a module integrated in a laptop computer or through the use of a smartphone.

Dixon's research, which is still ongoing, bears out many of these observations. Dixon and his team examined a number of options for network connectivity, including leveraging commercial networks and establishing virtual private networks, and as well as the efficacy of devices that could be used to provide cellular service to the battlespace. These options are being examined from the perspectives of effectiveness as well as costs.

The options considered for user devices included connecting a cell phone through a modular device and Ethernet cable to a tactical radio; customizing a cell phone to communicate directly with tactical radios; and upgrading tactical radios to communicate on both frequency bands simultaneously with two separate radio frequency chip sets and antennas.

Dixon then set about testing those concepts at a National Guard facility in California. "The first phase of the tests involved configuring the devices, to see what works with what," he said. "The second phase involved measuring throughput, detecting bottlenecks and testing security vulnerabilities."

Later Dixon convened a series of workshops through which various organizations within the armed services provided feedback. Industry representatives gave presentations at the invitational workshops.

While Dixon is still studying some of the issues involved, he assumes that costs will play an important role in making final decisions. On the other hand, the least costly alternatives will likely not satisfy military requirements for encryption, anti-jamming capabilities and network topology.

"For some missions, at least," he said, "you would need a military grade radio that has frequency hopping to prevent an adversary from locking onto the signal."

Although standard cell phones won't fill that bill, Dixon suggested that a sleeve could be developed into which a cell phone could be slipped, which would supply the phone with the requisite features and functionality. Dixon and his mentor, Professor Geoffrey Xie of the Naval Postgraduate School, are examining ways to make cell phones more secure by incorporating software encryption into the devices.

One of the purposes of Dixon's outreach through workshops was to acquaint vendors with the research so that they can start developing technologies to meet the needs of the military. "We also want to know what industry is working on," said Dixon. "Industry can develop products faster than the government. We also don't want there to be a duplication of effort."

Ownership, Policy Issues

Other issues that need to be hashed out before cellular technology can be introduced to the battlespace include those of frequency ownership. "You have to deal with that in each particular part of world where you are operating," said Ligas. "That is something the government has to manage. The government works with carriers like Sprint if it wants to use some spectrum in the United States."

IPWireless' strategy is to use spectrum bands that are not used commercially in most countries so that the military can safely operate on it. "We also prefer military applications to operate at relatively low frequencies, in the 600 MHz to 900 MHz range rather than Wimax's 3.6 GHz," said Quayle. "The reason is that military wants to maximize coverage. The lower the frequency, the better the coverage."

Policies that govern the adoption of technologies represent a potential barrier, according to Sprint's Ligas. "We work closely with all the service branches to make sure we meet their needs," he said. "As technology changes rapidly, the branches need to keep up with advancements and make sure they can use latest and greatest."

Ligas would like to see a unitary certification process for wireless devices that can be introduced throughout DoD. "At this point each of the service branches has its own separate testing processes for commercial applications," he said. "The procedures are different depending on whether you are dealing with the Navy, Air Force or Army to get a particular device certified. I believe DoD will eventually look at all device certifications for every type of wireless device and determine that if it is certified by some designated entity such as the Defense Information Systems Agency, then everybody can use it. There has been some talk of this. Not having to go through four testing processes would be advantageous."

The biggest sticking point, for Dixon, is what he terms "socialization," which involves the acceptance, or lack thereof, of a technology for military application by the leadership. "If senior military officers want this capability, they are going to have to push for it," he said. "The more the senior leadership looks at this technology and are educated on its capabilities and vulnerabilities, the better they can assess more quickly" what role it can play for the military.

A policy change that would allow these types of devices to be used by combatants will come naturally, according to Silberstein, as mobile devices are used more and more to access the Internet and as commanders use BlackBerry or similar devices.

"As applications grow and as the proliferation of wireless devices to access e-mail, the Internet and video continues" the more likely these devices will be accepted for use in the military, he said. "The greater speed of 4G will also be a benefit."

Dixon has already seen progress on the acceptance front. When he first started his research in 2008, none of the armed services boasted a program of record for the introduction of cellular technology. Now, he said, the Marine Corps and the Army both do. ✯

Contact Editor Harrison Donnelly at harrisond@kmimediagroup.com. For more information related to this subject, search our archives at www.MIT-kmi.com.