National DEFENSE NDIA
NDIA's Business and Technology Magazine

Communications

Rise of Smartphones May Sound Death Knell for Old Push-to-Talk Radios

January 2012

By Stew Magnuson

Push-to-talk radios — as generations of U.S. troops have known them — are on their way out.

Handing an infantryman a device the size and shape of a brick that can only perform one task, voice communications, may soon be akin to issuing him a musket.

The Army is pressing ahead with experiments that marry new software-defined radios to commercially available devices such as Androids and iPhones. But that is only an evolutionary step, military communications experts have said.

Manufacturers who supply the military with communication devices said they are preparing for the day when radios not only look more like the smartphones that have become ubiquitous in the civilian world, but perform a multitude of tasks.

Dennis C. Moran, vice president of government business development at Harris Corp.'s RF Communications group, said even the word "radio" may soon be outmoded. He prefers "network device" to describe what troops may be carrying into future battlefields.

"We acknowledge that this is the way the department is going and we are making the appropriate investments in products and capabilities," he said.

"What the soldiers, sailors, airmen, Marines are looking for is a rich, multi-media experience with some type of data device that gives them easy access to relevant operational and intelligence information," he added.

But it is not as simple as running down to the local Best Buy and snapping up a pallet of iPhones. Adapting commercial products for military use never is, said Niranjan Suri, a research scientist who is studying the issue at the Florida Institute of Human and Machine Cognition.

The consumer market has driven the development of devices that are small, with high-resolution displays, reasonably powerful storage and processing capabilities, and that are power efficient. They can also host a large number of applications that can be developed very quickly, Suri said at the Milcom conference in Baltimore.

What's not to love about them?

"If you talk to users in the DoD community, they will always ask, 'why don't I have this in my device?'"

There are multiple reasons why they don't, he said.

First and foremost perhaps is connectivity. Unless the device is connected to a network, it is useless. Smartphones were designed to work on commercial cellular infrastructures, which probably won't be available to troops in foreign lands. They also don't do point-to-point communications. In order to talk with a fellow squad member a few yards away, a soldier's transmission would have to travel back to a cell tower, then come back to their location.

Another major issue is security. The military has invested a great deal of resources to ensure that enemies can't intercept radio communications or jam their signals. That is not the case with commercially based phones running on Android or Apple operating systems.

There are also issues with the devices themselves. They must be rugged enough to operate in extreme conditions.

They can't employ exotic batteries. And their touch screens should work even if a user has dirty hands, there is excessive sun glare or he is looking at them with night-vision goggles.

And lastly, there are still questions to be resolved on tactics, techniques and procedures, Suri said. "What does using such a device do to war fighting operations? Will they be distracted looking down at their arm?" he asked.

Skeptics are also questioning whether every man in a platoon must have a multi-functional communication device. And if they do, what kind of applications will they need? No one is suggesting they be allowed to install Angry Birds, but what are the real requirements?

The Army has run several tests called the Network Integration Evaluations at White Sands Missile Range, N.M., and Fort Bliss, Texas, to address some of these questions. (See story page 35.)

In 1997, long before the word "smartphone" was coined, the U.S. military launched its Joint Tactical Radio System, the JTRS program, which is bringing software-defined radios to battlefields. These next-generation radios run on software programs called "waveforms."

In the Southwest desert exercises, the Army is experimenting with marrying smartphones to handheld Riflemen Radios that use the new soldier radio waveform. That is allowing the smartphones to "ride" on secure, established communications links without worrying about cell phone towers being in place, or other security concerns.

The problem is that development of the algorithms for these waveforms began before the explosion of mobile computing.

Lewis Johnston, vice president of advanced programs for Thales Communications Inc., said the soldier radio waveform was not designed to handle all the processing power needed to run a smartphone. The more processing power needed, the more energy a device consumes. Soldiers need to have reliable radios that don't run out of battery power mid-mission.

A better fit for running the applications found on smartphones is the wideband networking waveform, which was not envisioned to be on handheld radios sent out to the so-called "tactical edge." It requires a lot of energy to do the processing. It was intended for base stations or radios found in vehicles where they can rely on larger batteries.

"It hasn't got a practical implementation for the dismounted radio," Johnston said of the wideband waveform, but there may come a day when batteries become more efficient, and the waveform is improved so it is not so processor hungry.

Meanwhile, expeditionary units can address the connectivity issue by bringing their cellular network onto the battlefield. Companies are offering "bring-your-own" broadband wireless networks for expeditionary forces.

Lockheed Martin's MONAX system fits in two containers about the size of large trunks. The antenna gives users a range of about 38 kilometers, and can host more users than a typical commercial cellular tower.

"We typically don't jump into someone's country and trample on their cellular system anymore," said Patrick Opet, MONAX lead systems engineer. It operates on the little used 700-megahertz band of radio spectrum in order to avoid interfering with other cellular systems.

It is device agnostic and can link to all smartphones and tablets, he added. As for point-to-point communications, there are solutions to that problem. A unit could potentially carry a Wi-Fi hotspot with them. Even so, the system is still susceptible to jamming.

"That's why it would never replace singcars," Opet said of the Single Channel Ground and Airborne Radio System, the legacy push-to-talk radios that JTRS is expected to one day completely replace. "It is designed to be a complementary system."

Harris Corp., and partner Battlefield Communications Systems, has a similar offering, the NightHawk 3G, a cellular network designed for units that are on the move. It is being used now in Afghanistan, Moran said.

Other vendors are lining up to make sure they are part of the smartphone movement. Twisted Pair, a Seattle-based company, has a tactical 4G command center cloud that it says can tie all the legacy radios and smartphones together.

"It allows secure communication between any device, between any user over any network. It's removing that tether that says, 'I'm a radio, therefore I have to speak to another guy on a radio,'" said James Mustarde, director of marketing. It manages permissions in terms of who has the secret clearances to communicate with others.

"The device becomes almost irrelevant," he said. A person on a Cisco phone in the Pentagon can communicate with a soldier using a smartphone in the battlefield," he said. "You come to the table, you can eat off the table, as long as you have permission," he said. The Army and U.S. Special Operations Command are customers for the system.

As for making the devices rugged enough to survive the harsh military environment, it is not as easy as picking up a shock-absorbent rubber sleeve at a consumer electronics store.

HHCS Handheld USA Inc., a Corvallis, Ore.-based vendor of ruggedized smartphones and tablets, is already indirectly selling devices that meet military specifications to Defense Department agencies through prime contractors, according to Amy Urban, director of marketing.

“A lot of people assume we have taken a fragile computer and put it in a tough box. It’s much more complicated than that,” she said.

Commercially available items that buffer phones and tablets from shock give consumers some protection, “But for people who work outside day in and day out, that’s not even close to being good enough. There is no comparison.”

Devices must be hardened against dust and water, temperature shocks when going from a warm indoors to cold exteriors, and high altitudes that can affect the performance of electronics, she said.

Toughening them up takes away some of the weight advantages found in consumer phones and tablets. They end up being larger and heavier, she noted.

The company builds all its devices according to military specifications, no matter who the customer. “The nice thing about building for milspecs is that it translates very well for the general utility worker, police officer, forester,” she said.

The amount of security built into the commercial systems is also inadequate for the military.
Harris’ Moran said the National Security Agency has not yet articulated to industry the requirements for secret and below security architectures in a wireless environment. There is ongoing dialogue between industry and the NSA, he said, but until that is worked out, the widespread proliferation of smartphones on battlefields will be stymied.

“Once you solve the security problem in the secret and below in these data devices, I think you’re going to see a boom in the kinds of apps ... that can be loaded onto these data devices and that can go into the cloud,” Moran said.

There is a large potential market — both inside the military and out — for making mobile computing devices such as smartphones and tablets more secure. Senior officers who may be in garrison, but carrying sensitive information, as well as employees of government agencies and corporations need ways to secure their phones and tablets.

CACI has developed an end-to-end system that adapts tablets and smartphones for restricted use, said Scott Ference, principal systems engineer at CACI’s homeland security solutions information systems division in Eatontown, N.J. It tests potential applications for security vulnerabilities and has created an iTunes-like store where only approved software programs reside. Users cannot download an app unless it is in there.

The company can also “neuter” the devices according to an organization’s specifications. If cameras aren’t allowed in restricted areas, those can be disabled. A “sled” can go over the device to block the camera lens and 10-point connector. If the device is lost or stolen, or the user tries to remove the sled, the data on the device is wiped out.

“We jailbreak them. Take out the camera. Take out the Wi-Fi, and give the customer a new warranty,” Ference said.

Green Hills Software Inc. is offering embedded programs that walls off secure and non-secure parts of a smartphone. A mobile device can have a “dual persona,” said John Warther, vice president of government programs at the Santa Barbara, Calif.-based company.

“The problem is we’re trying to bolt on security just like we did in the Windows world,” he said.

Instead of trying to patch vulnerable apps, Green Hills’ system layers a separate operating system over the commercial device and partitions it off. This can be accomplished using a flashdrive without opening up the smartphone. So a user could have an unsecure program such as Angry Birds or Facebook on his phone, but they would never be connected to the secure portion.

Once the security and connectivity issues are settled, troops could have a multitude of different applications on their communication devices — everything from blue-force tracking to detailed maps.

A so-called “combat cloud” has enormous potential, Moran said. Those serving on battlefields will have access to a virtually endless amount of information that is not stored on their device.

For now, the “killer app” he has observed being used on the company’s NightHawk system is chat. This function allows soldiers to precisely text coordinates for fires, or the locations of medical evacuations.

Another is full-motion video — and to some extent — still pictures, that can be taken on the phones and sent back

to operating bases, where commanders can study them, he said.
Web services, the ability to download data or manipulate databases or webmail that resides in the cloud, is another potential killer app, Moran said.

Despite the endless possibilities that these applications may provide, "voice is still king," Moran stressed. It is too early to write the obituary for radio. It will always be a part of the suite on a multi-functional device.

There are still thousands of legacy singcars radios in inventories, and the new software-defined radios still have the "brick" look, although many are smaller. They will probably be in the military inventory for many years, but radio manufacturers already see a day when the bulky boxes with an antenna sticking out will be replaced by radically different "form factors" — industry jargon for the cases that hold the guts of the radios.

"It will be a single form factor where the individual soldier, sailor, airman, Marine will be focused on a screen," Moran predicted.

Thales' Johnston said there may not be any box at all. It could be something worn on the sleeve. The antenna and power source could be integrated into a uniform. The Army has already looked at some of these soldier system concepts in programs such as Nett Warrior, he noted.

There will always be some kind of over-the-air radio frequency interface, but all the information could be shown on heads-up displays similar to what military aircraft pilots see in their helmets, Johnston said.

Thales is not investing money in making smartphones, but continues to seek ways to drive down the size, weight and power consumption of radios, Johnston said.

"The concept of, 'I'm going to get rid of all my legacy and JTRS type stuff, and I'm going with a smartphone infrastructure,' that's a ways out," Johnston said.

Tom Rigsbee, U.S. federal government markets manager at Motorola, said as both a manufacturer of traditional push-to-talk radios and consumer phones, his company is well positioned to provide the ruggedized, secure devices the military and other agencies require.

"We're seeing from our customers a lot of interest in the form factor of the commercial devices. They like the physical attributes," he said. The challenge is making them durable and rugged.

The market is more about "expansion" than "evolution," he said. There are people who do not normally use radios, but now have a need for rugged, secure smartphones or tablets, he said. Motorola is investing in a "secure Bluetooth" system, which will encrypt the link between the earpiece and the smartphone.

Harris, Motorola and Thales all sell products to the domestic first responder radio market. Firefighters, police and other emergency management personnel are also looking to smartphones as a better way of communicating, company representatives said.

"I love the vendors. But they'll tell you anything," said Jeff Mercer, director of strategic communications for the joint program executive office JTRS.

That's why the Army is running the tests in New Mexico. It wants to see the purported solutions to these problems in action to see if they really work, he said.

As for the future of radio, the JTRS program that is attaching a smartphone to a Rifleman Radio is just an evolutionary step, he said. The office is already working to get rid of the cable that ties the pair together and to create a wireless connection between them.

The joint office is also getting out of the "box building business," he said. Military radio programs in the past spent too much time worrying about the casing, or the form factor, which slowed down programs.

As long it is running a JTRS waveform, it is interoperable. What shape these communications devices take in the future will depend largely on industry, he said.

"We're going to get out of that business and let industry — who does that well and is easily able to adopt new technology and incorporate it — do that for us," he said.

"It could be like a little pin on your lapel if industry is able to get it down to that size," Mercer said.

Reader Comments

Re: Rise of Smartphones May Sound Death Knell for Old Push-to-Talk Radios

Using commercial products on the battlefield is by no means a new practice with militaries around the world

beginning to exploit the potential of commercial off-the-shelf (COTS) solutions. The problem with a smart phone such as the iPhone is its suitability for the environment. On a physical level smart phones are obviously not robust enough to survive a military field operation, but they've also not been designed for military comms use, so safeguarding them with additional layers of security for example, will always require a process of retrofitting, as opposed to building from the ground up – never a good first choice. Canny suppliers are taking widely available COTS technology and fine tuning it in the manufacturing process to suit the sector in question. Our new satcoms device is based on commercial tech and uses the Iridium satellite network to provide secure AES256 beyond line-of-sight communications. It's IP67-rated, only 300g and boasts M2M-ready interfaces. It's light enough to be used as a battle-ready personal satcom device or as a secure data link to land, air or sea assets making use of a detachable antenna and its robust, versatile design. It also has an advanced commercial battery design which means it can send positional reports every 15 minutes for almost eight days. However, most importantly, the satellite carriers it uses can't be disrupted by in-country powers. GSM and GPRS can literally be switched off – and a smart phone is only as good as its network. Beyond line-of-sight (BLOS) comms is therefore the crucial factor to consider when debating the benefits of these devices in the field.

Giles Peeters
Track24 Defence Director
Canada

Giles Peeters on 01/03/2012 at 04:25

Submit Your Reader's Comment Below

***Name**

***eMail**

The content of this field is kept private and will not be shown publicly.

***Comments**

Please enter the text displayed in the image.
The picture contains 6 characters.

***Characters**

***Legal Notice**

NDIA is not responsible for screening, policing, editing, or monitoring your or another user's postings and encourages all of its users to use reasonable discretion and caution in evaluating or reviewing any posting. Moreover, and except as provided below with respect to NDIA's right and ability to delete or remove a posting (or any part thereof), NDIA does not endorse, oppose, or edit any opinion or information provided by you or another user and does not make any representation with respect to, nor does it endorse the accuracy, completeness, timeliness, or reliability of any advice, opinion, statement, or other material displayed, uploaded, or distributed by you or any other user. Nevertheless, NDIA reserves the right to delete or take other action

☐ I have read the Legal Notice.

Submit