Military tests usefulness of smart devices

September 27 2011, By W.J. Hennigan

As a Cobra attack helicopter pilot, Marine Capt. Jim "Hottie" Carlson was running support missions above Afghanistan last summer when it occurred to him that it was taking far too long to find where U.S. troops were under attack.

"Do you have any idea how long it takes to find the right map, unfold it, and find where you're going? It's agonizing," he said.

Frustrated that he had to flip through dozens of maps stuffed inside his chopper, Carlson, 31, loaded the documents onto his personal iPad, enabling him to zoom in, zoom out and quickly move from one map to another.

Carlson's brainstorm shortened the time it took to pinpoint a location from "three minutes to about 30 seconds," he recalled recently, and it soon helped change the way the military is thinking about warfare. The Marines now have more than 30 iPads in cockpits across their fleet of helicopters and fighter jets.

For soldiers in the 21st century, iPads, iPhones, Androids and other smart devices could eventually be as common on the battlefield as helmets, canteens and rifles.

These devices are being tested across all branches of the military. Seeing an opportunity, software companies and defense contractors are developing mobile applications that will enable soldiers to pass along intelligence, view reconnaissance images or even pilot small drones by remote control.

This high-tech hand-held revolution, of course, opens the military up to the same problems that everybody else with a smart device faces - security threats and concerns about dropped service. There are concerns among military strategists about passing military secrets on a device that can easily be hacked.

In years past, the Pentagon probably would have spent billions of dollars creating its own custom devices, but modern technology offers a much cheaper alternative, said Michael McCarthy, who leads an effort by the Army to test smartphones for use on the battlefield.

The Army is using iPhones, Androids and BlackBerrys in mock wartime situations in New Mexico and Texas.

Such devices are coming in handy in simulated security raids and checkpoint stops to take pictures of Arabic writing and gather biometric data, such as fingerprints and iris scans, McCarthy said.

"It's all about information gathering, and tools to make the job easier," he said.

The troops are also testing about 95 mobile applications, or apps, designed to help soldiers perform specific tasks with their cellphones. One app is dubbed Soldier Eyes. "Imagine that you're dropped in an unknown location on a moonless night," McCarthy said. "You open this app and through its GPS coordinates, it shows you where you are. It shows you where your adjacent units are."

It can also provide cumulative information about the region, he said, showing how many roadside bomb attacks have occurred and when they took place.

The app is being developed by Overwatch Mobile Solutions, a subsidiary of Textron Inc., in close collaboration with the Army.

"A typical soldier carries a map, a compass, a radio and a GPS," said Evan Corwin, a senior program manager at Overwatch. "This enables them to have all of that on one device."

In all, the Army said it has spent about $4.2 million over two years to develop the apps and test smartphones.

The Air Force and Navy also have pilot programs testing smart-device technology. But the devices are risk-prone and susceptible to security breaches that could threaten military secrets.

Internet security firm McAfee Inc. recently found that malware, short for "malicious software," targeting smartphones and tablets is on the rise.

The widespread adoption of mobile devices is likely to bring about "an explosion" of attacks, McAfee said.

"Given our historically fragile cellular infrastructure and slow strides toward encryption, user and corporate data may face serious risks," the company said.

Critics wonder what will happen if a soldier's Android is hacked or infected with malware.

"The military is opening themselves up to serious problems," said Chris Soghoian, a privacy and security researcher at the Center for Applied Cybersecurity Research at Indiana University. "It seems stupid to use a platform that thousands of people are trying to hack."

Storing data on the phones will end up disclosing military information or showing the enemy precisely where the troops are through the devices' GPS transmitters, Soghoian said. "It's a recipe for disaster."

Symantec Corp., known for its personal computer security software, is developing a product called O3 that officials say could secure wireless military networks. Much of the company's planning will depend on how the Army wants to proceed on smartphone security.

If the Army was to decide to put a smartphone in the hands of every soldier, it alone would need to buy 1.2 million phones. That could be a major source of revenue for phone makers.

In the coming years, defense giant Raytheon Co. anticipates that the app market will be huge. The company, famous for building 2,000-pound bunker-busting bombs and Tomahawk cruise missiles, will unveil an online store called Appsmart this year where military apps can be bought.

"We think that within three years there will be a major move in the military toward fielding mobile handsets," said Mark A. Bigham, Raytheon's vice president of business development for defense and civil mission solutions. "We hope Appsmart will play an important role in that initiative."

Commercial apps typically sell for a couple of dollars because they often sell by the millions. With far fewer made, military apps are expected to be more expensive and could sell for as much as $500 apiece, Bigham said.

The company has developed the Raytheon Advanced Tactical System, software that enables troops to share sensitive information on smartphones. It has also developed more than 20 apps. "There's a lot of companies large and small vying for this marketplace," he said.

Harris Corp. of Melbourne, Fla., has developed a miniature cell tower mounted on a Humvee that provides cell coverage to remote areas with patchy or nonexistent service. The system, named KnightHawk, generates connectivity by providing network signals for a three-mile radius.

"Troops aren't typically dropped in an area where AT&T and Verizon have coverage," said Edward J. Zoiss, Harris' vice president of advanced programs and technology. "That's where Harris comes in."

The company, which also makes military radios, believes that the services will use smart devices at the front lines in battle, and that KnightHawk will provide coverage. Harris has also developed an app called Eyes-on-Target that enables troops to share streaming video on their phones - rather than use radios and hand and arm signals.

Even drone aircraft may get a boost from these phones. Students at MIT and researchers at Boeing Co. have demonstrated that a person can fly miniature drones with an iPhone.

Imagine a soldier pulling a drone out of a backpack and then controlling it to see inaccessible spots on the battlefield, said Boeing technician Joshua Downs. "It is applications such as this that are helping to move the technology forward."

Citation: Military tests usefulness of smart devices (2011, September 27) retrieved 25 April 2024 from https://phys.org/news/2011-09-military-smart-devices.html