

# Wireless World: Clandestine communications

March 3 2006

---

New wireless technologies being developed by a secretive government agency in collaboration with private contractors may dramatically improve communications for homeland defense among federal, state and local officials, experts tell United Press International's Wireless World.

The Department of Homeland Security, working with BlackBerry Wireless devices, Palm Treos and other mobile handheld computers, has been working to secure wireless e-mail through a testing program being run by its very secretive Advanced Research Projects Agency, a unit created for the war on terror that is analogous to the Defense Advanced Research Projects Agency, devised during the Cold War by the Pentagon to create secret, new technologies.

The project by Homeland Security's ARPA has been sending 1,000 e-mail messages a day, wirelessly, linking DHS and the Royal Canadian Mounted Police. This summer the project will start sending the e-mail communications via satellite -- and begin to integrate the technologies into the infrastructure of the government.

Staying in touch by wireless e-mail has become essential during a national disaster, just as it is during routine operations, experts tell Wireless World.

"E-mail has become the most used communications technology in organizations, even more than the phone," said Marty Hollander, vice president for marketing at Cemaphore Systems Inc., a disaster-recovery

company based in San Mateo, Calif. "E-mail is the way work gets done because it combines both real-time delivery with the richness of physical delivery."

But mobile communications can go down during a disaster -- like Hurricane Katrina -- or during an attack, like the terrorist onslaught on Sept. 11, 2001, when panic in New York and Washington overwhelmed mobile-phone lines.

One way to keep the networks online being pushed by some technology developers is so-called mobile mesh networking technology, which is based on a combination of mobile technologies and can be deployed very quickly when conventional mobile lines go down. "After Katrina and Rita, Intel and Tropos donated over 100 units for deployment in the Gulf region," said Ron Sege, chief executive officer of Tropos, a wireless network developer.

The problem: The deployment was not immediate. "Thirteen Tropos metro mesh networks were deployed in three states in less than three weeks," said Sege.

While that performance would be considered spectacular during normal business operations, the government wants to ensure that they never lose communication with any other agency, whether it is on the federal, state or local level, during a disaster.

That's the primary reason why DHS is looking at satellite communications to supplement cellular networks -- and keep the wireless e-mail and voice comms flowing during a crisis.

A spokesman for World Communications Center, a satellite-phone provider, tells Wireless World that users look to satellite telephony for Internet and data transfer when regular phone lines fail. On Monday the

company will announce news about an emergency-response project that relies on Iridium-based mobile telephones, which can help government and business set up emergency "command centers" after a disaster.

Some developers are examining the use of "legacy" government satellites -- no longer needed military sats -- to create networks for emergency communications purposes. Recent tests of X-band service, using military legacy equipment, has demonstrated data rates that are in excess of 100 Mbps, according to XTAR LLC, a joint venture of Loral Space & Communications and HISDEAT.

That's only part of the spending story, however. The government is dedicating nearly half of all new IT spending for fiscal year 2007 for homeland security, or more than \$4.4 billion, according to the research group Input.

Is there a possible danger to individuals' free speech if the government takes over all communications networks, as some civil-liberties groups might argue? Does anyone really care anymore? Not many Americans even seem to be able to name more than one of the five fundamental freedoms granted to them by the First Amendment of the Constitution, according to a survey released this week by the McCormick Tribune Freedom Museum in Chicago. "Many Americans don't have an understanding of the freedoms they regularly enjoy," said Dave Anderson, executive director of the museum.

The government, meantime, seems likely to continue to seek ways to control access to the means of communications in the name of homeland security during the ongoing war on terror. "No one should lose his or her life because public safety officials cannot communicate with one another," said Rob Drake, mayor of Beaverton, Ore., in testimony this week before the House Homeland Security Subcommittee on Emergency Preparedness, Science and Technology, adding that this week marked

the third anniversary of the creation of the Department of Homeland Security.

*Copyright 2006 by United Press International*

Citation: Wireless World: Clandestine communications (2006, March 3) retrieved 25 April 2024 from <https://phys.org/news/2006-03-wireless-world-clandestine.html>

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.