ArmyTimes

Army: Working to encrypt UAV video feeds

By Michael Hoffman, John Reed and Joe Gould - Staff writers
Posted : Monday Dec 21, 2009 7:30:25 EST

The Army is scrambling to protect the live video feeds from its unmanned aerial vehicles from being intercepted by the enemy. Raven drones will be retrofitted with encryption technology as early as this month.

Defense officials confirmed Dec. 17 that Iraqi insurgents have been capturing the nonsecure, line-of-sight communications signals from Army and Air Force drones since mid-2008.

Army officials acknowledged that the service has fielded hundreds of drones without the ability to encrypt the signals that ground forces rely upon for intelligence and surveillance of insurgent hideouts or roadside-bomb hot spots.

However, the Army will retrofit the handheld Raven and other UAVs over "at least two years," targeting currently deployed systems first, said Col. Gregory Gonzalez, the Army's project manager for unmanned aerial vehicles.

For the Shadow, Hunter, Warrior Alpha and the Extended-Range Multipurpose UAV, the Army will retrofit all systems with encryption, as funding permits, said Gonzalez.

"This is not the first time that we have heard about the potential threat against full motion video. The threats are ongoing, and the Department of Defense has taken some risk," said Gonzalez. "We received specific direction from the Office of the Secretary of Defense within the last year to fix the problem."

A report published in the Dec. 17 edition of The Wall Street Journal detailed how defense officials earlier this year discovered laptops in Iraq loaded with a $26 Russian-made software program called SkyGrabber that hacked into video broadcast by Predator cameras, which show the location of insurgents being targeted by the drones.

Besides the SkyGrabber software, insurgents have used high-tech methods to capture the video feeds.

U.S. troops found advanced electronic warfare equipment in a 2008 raid on Shiite militia, according to an Air Force intelligence officer briefed on the raid.

Army officials acknowledged the interceptions, and the Pentagon issued a general statement on the security of its intelligence gathering.

"The Department of Defense constantly evaluates and seeks to improve the performance and security of our various ISR systems and platforms. As we identify shortfalls, we correct them as part of a continuous process of seeking to improve capabilities and security," the statement said.

One Air Force official contends the insurgents' ability to watch drone feeds has adversely affected U.S. operations in the Middle East.

"We noticed a trend when going after these guys; that sometimes they seemed to have better early warning" of U.S. actions, said the officer briefed on the raid. "We went and did a raid on one of their safe houses and found all of this equipment that was highly technical, highly sophisticated. It was more sophisticated than any other equipment we'd seen Iraqi insurgents use."

The militia, known as Kata'ib Hezbollah based out of Sadr City, Baghdad, has long been suspected of being a surrogate for Iran's Quds Force, the wing of the Iranian Army responsible for conducting clandestine warfare outside of Iran via various insurgent groups.

"It was the technological know-how to make the antennas, computers and software go together and pick up the appropriate bands that was impressive," the officer said.

Soon after the raid, top commanders in Iraq convened a task force to identify the extent of the threat and how best to deal with it, according to the officer. Initial findings showed the threat was isolated to Kata'ib Hezbollah.

"They knew that we were flying Predators over their heads 24/7, so it's easy to say, 'yeah, I know that I'm going to do a signals analysis search for [the drone] and take advantage of it," the officer said.

The laptops loaded with the SkyGrabber software also had footage filmed by

smaller Army UAVs as well as the Predators.

“We are well aware, and [Office of the Secretary of Defense] is well aware, and we have a well-researched response set in motion,” said Col. Robert Sova, the Army’s capability manager for unmanned aerial systems. “This ability, this is not new information.”

Ground units get the Predator feeds through a Remotely Operated Video Enhanced Receiver, or ROVER, — a mobile device that looks like a laptop that can either be carried by hand or mounted in a ground vehicle.

An encryption package can be added to the ROVER; however, not all troops have the encryption package. The latest ROVER model being tested by the Pentagon comes equipped with two advanced encryption packages.

The military has not implemented encryption for drones for “various reasons,” according to Sova.

But, Sova said, the ability to hack a drone’s video feed is a “very low risk” since the insurgents haven’t figured how to hack into the command and control systems of the drones.

“It’s not like they’re going to control the payload or move it off,” Sova said. “They’re able to see a specific interval, like a camera system in the mall.”

Sova considers it unlikely that an insurgent could tap into a specific drone overhead.

“It’s happenstance, if they were able to tap into that feed,” Sova said. “Only in the best scenario, and only for a short period of time.”

The Defense Department’s Office of Acquisition, Technology and Logistics directed the services to beef up encryption. Prior to his departure last year, Pentagon acquisitions czar John Young oversaw such a push, across all services, according to Gonzalez.

“Since these systems were first introduced, we’ve known [the risks of unencrypted video feeds],” Gonzalez said. “Your average off-the-street person isn’t able to get these feeds, but with enough effort you can. The risk to the Department of Defense seemed low. Now, for whatever reason, the Office of the Secretary of Defense has decided to reduce that risk.”

According to Gonzalez, by the first of the year, the Army will field encryption-capable Ravens, and other UAV systems will follow over the coming months and years.

“The priority is to give it to every unit in theater or going into theater, so that they will have encryption,” said Gonzalez. “The whole process will take a year, and within a year, several units will have encryption.”

Air Force officers and defense analysts caution that video broadcasts from manned aircraft to U.S. ground troops are vulnerable to hacking as well because they have technology similar to that of UAVs.

The Air Force has known for more than a decade that the live video feeds from its unmanned aerial vehicles can be intercepted by the enemy but opted not to do anything about it until this year. An official document puts a completion date to secure the feeds at 2014.

The Air Force first flew the RQ-1 Predator, the MQ-1’s predecessor, in combat over Bosnia. In published reports, local residents with satellite television told of watching Predator video feeds on their televisions.

Defense analyst Peter Singer, author of “Wired for War: The Robotics Revolution and Conflict in the 21st Century,” said, “I remember that some of the people there said it was harder to get the Disney Channel than watch U.S. military operations.”