

Army Works to Build and Maintain Intel Capabilities in Cloud

By Jared Serbu, Federal News Radio, December 27, 2011

Over the last decade of war, the Army says it's learned a lot about how to leverage technology to put intelligence into the hands of soldiers. Leaders are trying to make sure they don't lose that momentum once soldiers are off of the battlefield.

The Army is pressing ahead with the development of a cloud-based solution for intelligence collection and analysis designed to replace and integrate several preexisting systems, with the goals of getting intelligence directly to the battlefield quickly and efficiently.

The Distributed Common Ground System - Army, or DCGS-A, has been in the works for several years, and the Army is trying to make sure the momentum of its development doesn't slow down.

The overarching goal, said Mary Lynn Schnurr, the chief information officer for Army Intelligence, is to make sure intelligence isn't just in the hands of commanders, but rather instantly available and accessible to soldiers at the tactical edge, for instance, when they come across documents or digital data that they need to analyze quickly.

"Soldiers, when they go on a raid and they pull that pocket litter out, they want to be able to look at those phone numbers and find linkages, and they want to be able to do it right away," she said at AFCEA NoVa's recent Army IT day. "So we've put tools in place like TSETS, tactical site exploitation tools, that allow them to do exploitation right at the pointy end—right at the place of capture."

Other intelligence capabilities developed during wartime include radar that can sense through walls and 3G wireless networking to dismounted soldiers.

"It shows how much we've learned from the quick reaction capabilities (QRCs) we've put out there in the last decade," she said. "We have to move those into enabling programs of record, so that they don't fall off. So that the next time we have a serious situation we don't have to start all over again and start developing QRCs again. We have to start taking things that work well and move them into the future and sustain them."

The Army has been rolling out a third version of DCGS-A, which comprises of the Army's share of the broader Defense Intelligence Information Enterprise (DI2E). The latest version is designed to fix some serious shortcomings identified by intelligence commanders in Afghanistan in 2010, who complained that intelligence personnel still lacked the ability to tie together the overwhelming sea of information housed in a vast number of databases.

The system included the military's first tactical cloud, which came online in Afghanistan in March of 2011. The cloud, Schnurr said, forms the foundation layer of the intelligence gathering system. It helps store, aggregate and analyze data, with the objective of making that information available to any piece of widgetized software—built around a common architecture—that can make use of it.

Schnurr said that while the Army indeed wants to modernize its network infrastructure, its current efforts are not cloud for cloud's sake.

"The bottom line for us has to be on the outcome," she said. "What can we get from the cloud? The key is access. It's all about the data. Accessing the data from a myriad of sensors out there at all of those layers. And a cloud is not a cloud is not a cloud. We're really focused on a data-intensive, algorithmic cloud. And we're leveraging and taking advantage of everything out there in the intelligence community. We don't want to start something that others are already doing and doing pretty well."

For instance, for geospatial data, the Army wants to use the National Geospatial Intelligence Agency as its provider, and the National Security Agency for cryptological help. The system already is taking in data from the

Defense Intelligence Agency and the Marine Corps, and as of now, DCGS-A provides access to 53 million records from 317 data sources.

The next steps, between now and 2014, will be the integration of an app mall where intelligence users can hand-select the widget-type applications that work for them, taking advantage of real-time data provided by DCGS-A and providing access to that data based on attributes about particular users.

"We have to move from where we operated in the past, stovepiped environments, very hardware-centric, into the software-centric environment. That's a way that we can achieve some great efficiencies: by changing the model we operate in," she said. "We're just going to continue to enhance what we're doing today, getting more mobile apps out there, building that app mall, and just getting soldiers what they need rapidly. We're talking 30, 60, 90-day development cycles."

But tops on the to-do list is better security, particularly around insider threats. Schurr said the Army needs a robust suite of auditing tools so that officials can be alerted in cases where users are employing Army systems to view intelligence information they don't have a justification for accessing.

"We all know some of the very, very tragic incidents that have happened over the past couple years," she said. "We need to know when somebody who's not a China analyst is in the system in the middle of the night downloading 20 megabytes of information on China. When WikiLeaks happened, we had regulations and rules in place. They just weren't being followed. It's a people problem that's very easily solved, coupled with technology."