

## **Army Fights to Overcome Data Onslaught**

Distributed Common Ground System-Army constitutes DOD's first tactical cloud computing node

*By Greg Slabodkin*

*Defense Systems*

*Aug. 16, 2011*

When Army Maj. Gen. Michael Flynn took over in June 2009 as the top U.S. military intelligence official in Afghanistan, he was on a mission to shake things up in the intelligence community. Just six months into his new job, Flynn co-authored a highly critical report published by the Center for a New American Security, recommending sweeping changes to intelligence operations in Afghanistan, which according to the report were "only marginally relevant" preventing pivotal information from making it to those who needed it most.

Then, in July 2010, Flynn issued his coup de grace - a scathing Joint Urgent Operational Need (JUON) statement - warning that intelligence analysts in theater did not have the tools required to fully analyze the tsunami of data being thrown at them. This shortfall, he argued, prevented analysts from providing U.S. and coalition commanders with a full understanding of the operational environment in Afghanistan, resulting in missed opportunities and loss of lives.

Flynn's JUON was an urgent request for help in the form of a "theater-wide web-based advanced analytical platform to store, organize, access, retrieve and enable full understanding of intelligence and information from multiple large disparate data sets." Answering the call was the Distributed Common Ground System-Army (DCGS-A), the service's cornerstone system for intelligence processing, exploitation and dissemination, said Army Col. Charles Wells, DCGS-A project manager.

### **Griffin takes flight**

The latest version of DCGS-A, Version 3, called the Griffin software build, was fielded to Afghanistan in direct response to Flynn's JUON request for advanced analytics. Wells said that the Army "surged" the Griffin software capability, which has a modern web interface, to units rotating into Afghanistan to arm them with analytic tools needed to support the intelligence mission.

According to Wells, Griffin's operational impact in Afghanistan has been significant, including providing intelligence analysts with tools to perform link, pattern, geo-temporal, and enhanced graphical analysis; human intelligence reporting, source management, collection/asset management; access to biometric data; full-motion video exploitation capability; and incident prediction of improvised explosive devices and other events.

In addition, the Griffin software ties into a cloud-computing node that arrived at Bagram Air Base, Afghanistan, in November 2010 and went operational in March. DCGS-A Version 3 has the notable distinction of being DOD's first tactical cloud computing node.

Wells said that intelligence data generated in Central Command's area of responsibility, which includes Afghanistan, is growing at a "geometric rate." To handle the data onslaught, DCGS-A takes sensor data from all its sources - signals, imagery or human intelligence - and brings it all together as a common data format in a fused environment, making multisource intelligence analysis possible.

When Wells met with Flynn in Kabul in September 2010, the military intelligence chief emphasized to the colonel the vital importance of ensuring sharing of intelligence, surveillance and reconnaissance (ISR) data among the more than 40 coalition partners engaged in operations in Afghanistan. As a result, the Griffin software includes the DCGS Integrated Backbone (DIB), which supports real-time ISR data query and retrieval capabilities across coalition and security domains, giving coalition partners the ability to query U.S. intelligence data while also providing U.S. analysts access to coalition data.

Ironically, U.S. forces are in most need of the DIB.

### **First DIBs**

The Army, Navy, Air Force and Marines are each pursuing their own versions of DCGS, and although the services can share limited intelligence data, their progress toward full information sharing across the DOD enterprise has been uneven, according to the General Accountability Office.

Initiated in 1998, DCGS was envisioned by DOD planners to be an interoperable family of systems that would enable military users from across the services to access shared ISR information. The DIB is central to DOD's DCGS effort to enable seamless, real-time, multiagency intelligence sharing and collaboration.

To facilitate the sharing of ISR data, DOD developed the DIB to provide common information standards and protocols. At the heart of the DIB is a metadata catalog that allows users to access information via search engines like those on the Web. Using criteria such as key word, target information, product type or location, users can search through catalogs of information.

The problem, according to the GAO, is that DOD has not developed overarching guidance, such as a concept of operations that provides direction and priorities for sharing intelligence information within the defense intelligence community.

"Without this overarching guidance, the services lack direction to set their own goals and objectives for prioritizing and sharing ISR information and therefore have not developed service-specific implementation plans that describe the prioritization and types of ISR data they intend to share," the

GAO found in 2010. "Moreover, the inability of users to fully access existing information contributes to the increasing demand for additional ISR collection assets."

The DIB allows new intelligence entering the system to be identified, categorically tagged and incorporated into a database. However, in March 2010, Davi D'Agostino, GAO's director of Defense Capabilities and Management, testified before the House Armed Services Subcommittees on Air and Land Forces and Seapower and Expeditionary Forces that the services have not completed the process of prioritizing and tagging the data they want to share in accordance with these standards and protocols or developed timelines to do so. As a result, the services are not sharing all of their collected ISR data.

"Although the Air Force has the capability to share some Air Force-generated ISR information with other DOD users through the DIB standards and protocols, it has not developed timelines or taken steps to prioritize the types of additional data that should be shared with the defense intelligence community," D'Agostino testified.

Likewise, he said the Army also has the capability to share some of its intelligence data with other users, "but has experienced difficulties tagging all of its data because of its large inventory of legacy ISR systems." In addition, the Army has not established timelines for sharing data.

"The Navy and Marine Corps are not currently tagging all of the ISR data they intend to share and have neither developed timelines nor taken steps to prioritize the types of data that should be shared with the defense intelligence community," according to the GAO.

Nevertheless, Lt. Col. Thomas Tschuor, director of the DCGS Multi-Service Execution Team Office at the Electronic Systems Center, Hanscom Air Force Base, Mass., sees progress being made.

"Over the last six months, we have seen 100 percent growth in the number of operational federated nodes, and more nodes are coming online," Tschuor said, with the latest DIB version being incorporated into DCGS sites worldwide belonging to the Army, Navy, Air Force, Marine Corps, Special Operations Forces and the intelligence community.

For Air Force DCGS, in particular, the DIB is being used to federate with Army organizations within and outside the continental United States, he said.