IMINT Processing Problems Impact War on Terror

by Anthony L. Kimery

Monday, 26 April 2010

'We have always collected way more information ... than analysts can handle'

Addressing attendees of the “outside the beltway” GeoInt 2009 Symposium in San Antonio last October, Lt. Gen. David Deptula, Air Force deputy chief of staff for intelligence, surveillance and reconnaissance, began by emphasizing that the panoply of imagery intelligence that’s playing a critical role in pinpointing terrorists and prosecuting the war on terrorism around the world, “is going to become even more important as we move into the future.”

More than four months later, the Government Accountability Office (GAO) warned Congress that the Intelligence Community’s (IC) abilities to collect and analyze imagery from the myriad spy collection platforms is plagued by serious processing deficiencies that IC sources told HSToday.us has already caused problems in the overseas war on Al Qaeda and Associated Movements, or AQAM.

While this imagery intelligence (IMINT) has unquestionably been valuable in locating individual terrorists and terrorist training facilities, safehouse, etc. “there’s just so much of it – some of which needs to be correlated to other intelligence like SIGINT and HUMINT, that we just can’t process all of it as quickly as it many times needs to be. And we’ve got pipeline problems with more and more [of this intelligence] being downstreamed to us,” a veteran IC counterterrorist intelligence analyst familiar with the problems told HSToday.us.

The GAO told the House Committee on Armed Services’ Subcommittees on Air and Land Forces and Seapower and Expeditionary Forces on March 17 that the capabilities to gather imagery intelligence, or IMINT, is outpacing not only the ability to transmit the data to ground stations, but is overwhelming the number of IMINT analysts to effectively process it.

“The military services and defense agencies face long-standing challenges with processing, exploiting, and disseminating data from numerous intelligence, surveillance and reconnaissance (ISR) systems - including manned and unmanned airborne, space-borne, maritime and terrestrial systems - that play critical roles in support of current military operations,” lawmakers were told by GAO’s Davi M. D’Agostino, director, defense capabilities and management.

With regard to tracking Al Qaeda via Predator UAVs, GAO testified that only about half of all the intelligence that’s siphoned by a single Predator is capable of being fully exploited. There is so much digital data that it’s overwhelming the IC’s myriad processing capabilities.

Being able to quickly and effectively synthesize the tsunami of imagery - including full-motion video (FMV) - that’s being collected today from UAVs with the dizzying onslaught of SIGNIT and HUMINT, and then getting it disseminated to the people who needed it yesterday, has become one of the major challenges for both the military and the IC, especially as they prosecute the war on terrorism.

“We’re going to find ourselves in the not too distant future swimming in sensors and drowning in data,” Deptula said.
Some IC authorities say that has already happened.

With regard to tracking terrorists, especially in real-time using FMV, for example, you’ve got to have enough trained analysts to physically monitor all the disparate video streams - and there could be lots of them depending on the circumstances.

Also speaking at the GeoInt conference, Maj. Gen. Bradley Heithold, commander of the Air Force Intelligence, Surveillance and Reconnaissance Agency at Lackland Air Force Base and the Air Force geospatial intelligence element commander and commander of the Service Cryptologic Component, said tracking and killing Abu Musab Al Zarqawi, the leader of Al Qaeda in Iraq, in 2006 involved Predators flying 24/7 for a week before counterterrorists were able to zero in on his location.

“It’s a huge effort to find where [the terrorists] are,” Heithold said.

Heithold told Defense Systems that “you’ve got FMV and/or SIGINT coming off the platform,” thus “somebody has to have the full-time job of watching that FMV frame by frame, identifying threats, building patterns of life and fusing that with other sources of intelligence, such as imagery and signals intelligence from U-2s and Predators so that it is actionable by our ground forces with a high degree of confidence.”

“We lose a lot of data simply because the collector (or the owner of the collector) feels that the information is not needed or not valuable enough to keep.”

But with analysts in many instances needing to quickly weld imagery, SIGINT and other intelligence together, officials like Deptula have said the process will somehow have to be automated.

Harris Corporation has developed video image analysis systems designed to rapidly go through huge amounts of video, and is working to relieve the imagery data overload and processing problems by installing advanced broadband data links on UVA surveillance intelligence collection platforms, thereby “allowing [users] to more effectively handle the increase in data coming in,” a Harris fact paper stated. “The company is also providing advanced battlefront soldiers with handheld video viewers that enable them to see live UAV feeds coming in around them … helping to make immediate use of the imagery instead of having to wait for some type of analysis to be done.”

“Among the crucial problems recently cited by the GAO is the lack of processing capability for the enormous amount of data that's being collected, and the consequence inability for the limited number of experienced and qualified IMINT and other analysts to effectively exploit all this data,” HSToday.us was told by former naval intelligence officer, aviator and Force Protection/Anti-terrorism Officer Lani Hay, founder, president and CEO of Vienna, Virginia-based Lanmark Technology.

But “we have always collected way more information, with every collection platform, than analysts can handle,” Hay said, adding, “we lose a lot of data simply because the collector (or the owner of the collector) feels that the information is not needed or not valuable enough to keep.”
Hay has more than a decade of experience in military intelligence and is an acknowledged expert on reconnaissance operations and overhead collection assets and a recognized tactical intelligence expert in European, Middle Eastern and Far Eastern military operations. She spearheaded, researched and evaluated new exploitation techniques providing advanced development support for state-of-the-art prototype reconnaissance equipment.

“Another factor related to ‘too much data’ is the mission focus of collection,” Hay said. “A lot of raw information is collected in support of mission units who are enroute to the target and need ‘over watch’ or ‘tipper’ support in order to verify targets or provide that final force protection support up until the target is engaged and the force recovers. So all of that data, SIGINT/IMINT/ELINT is collected, and in a lot of cases just dumped, because the ‘next step’ of ‘who else needs to know,’ or ‘who else may benefit’ from this data, is not initiated. In some sense it is processing capability, however, there is a lot of ongoing effort to develop tools/databases/virtual storage, data movement/sharing as well as applications to provide the analyst ‘one view’ to the data.”

Hay said “the analyst actually has a lot of power/input into the development process because developers routinely get their requirements straight from the end user. This aspect can be a double edge sword, because no two analysts are going to like the same things and there is a lot of room for subjectivity.”

Continuing, Hay said “the Intelligence Community has developed a ‘community data layer’ in an attempt to address this issue of ‘too much data.’ Also, policy has been written that essentially says ‘need to share/make available’ vs. ‘need to know,’ which was a watch phrase that drove compartmentalization and non-sharing and was really a response to espionage losses such as the [John] Walker case, where Walker basically had free access to all the classified information on his ship and was never questioned. The ‘need to know’ policy basically put a stop to that ‘open and free’ access policy.”

“So how do we achieve ‘open and free’ access while still protecting not only the classic ‘sources and methods’ but the data itself?” Hay asked. “That is the policy/procedure and SOP issues facing the Intelligence Community today. Technology is almost never the driver (or rather the road block). Usually it is policy that is holding back the implementation of newer/better faster technologies and tools that the analysts can use. Organizational culture can have an impact as well.”
“Another thing, and we can see this quite well with biometrics,” Hay said, “is that typically we can stand up a capability to collect very quickly,” but “it's the analytical effort that takes time to come to fruition and provide a perceived ROI on all the data collected as well as resources expended to support that. Usually the analytical effort comes in second as far as resourcing vs. the collection effort.”

“Since 2002, DOD has rapidly increased its ability to collect ISR data in Iraq and Afghanistan, although its capacity for processing, exploiting and dissemination is limited,” GAO’s D’Agostino told lawmakers. “Second, transmitting data from ISR collection platforms to ground stations where analysts process, exploit, and then disseminate intelligence to users requires high-capacity communications bandwidth.”

“However,” D’Agostino pointed out, “bandwidth can be limited in a theater of operations by the satellite and ground-based communication capacity, and this in turn affects the ability to send, receive, and download intelligence products that contain large amounts of data.”

Further complicating matters, D’Agostino told the congressional panel that “shortages of analytical staff with the required skill sets hamper the services’ and defense agencies’ abilities to exploit all ISR information being collected, thus raising the risk that important information may not be available to commanders in a timely manner.”

D’Agostino said “DOD is developing and implementing initiatives to enhance its processing, exploitation, and dissemination capabilities, such as increasing personnel, but its initiatives are in the early stages of implementation and it is too soon to tell how effective they will be in addressing current challenges.”

Meanwhile, “DOD is taking steps to improve the sharing of intelligence information across the department, but progress is uneven among the military services,” D’Agostino said.

Seven years ago, in April 2002, the Congressional Research Service (CRS) noted in its report, Imagery Intelligence: Issues for Congress, that “beyond bureaucratic concerns, [the DOD even at that time] has far to go in being able to exploit the vast quantities of data collected” from IMINT assets, including UAVs.

The July 2004 Senate Select Committee on Intelligence Report on the US Intelligence Community’s Prewar Intelligence Assessments on Iraq, stated that “as with the other intelligence disciplines, there was a coordinated effort within the IC to improve imagery collection against the WMD target. The [CIA Collection Concepts Development Center, CCDC] study found that imagery assets were in high demand for the Iraq WMD target and for support to military operations,” which required “imagery assets to be tasked more efficiently and effectively. The CCDC study made several recommendations aimed at overcoming the challenges of competing [IMINT] priorities …”

In January, GAO told lawmakers in its report, Unmanned Aircraft Systems: Comprehensive Planning and a Results-Oriented Training Strategy Are Needed to Support Growing Inventories, that “DOD continues to increase UAS inventories, but in some cases, the Air Force and the Army lack robust plans that account for the personnel, facilities, and some communications infrastructure to support them. Regarding personnel, the Air Force and the Army have identified limitations in their approaches to provide personnel
to meet current and projected UAS force levels, but they have not yet fully developed plans to supply needed personnel.”

“Although DOD … requested funding and plans to request additional funds, the Air Force and the Army have not completed analyses to specify the number and type of facilities needed to support UAS training and operations,” the January GAO audit report stated.

Continuing, the GAO report said that “having identified a vulnerability to the communications infrastructure network used to control UAS missions, the Air Force is taking steps to mitigate the risk posed by a natural or man-made disruption to the network, but has not formalized a plan in the near term to provide for the continuity of UAS operations in the event of a disruption.

“While DOD guidance encourages planning for factors needed to operate and sustain a weapon system program in the long term, several factors have contributed to a lag in planning efforts, such as the rapid fielding of new systems and the expansion of existing ones. In the absence of comprehensive planning, DOD does not have reasonable assurance that Air Force and Army approaches will support current and projected UAS inventories. The lack of comprehensive plans also limits the ability of decision makers to make informed funding choices.”

The January GAO audit report pointed out that “DOD has not developed a results-oriented strategy to resolve challenges that affect the ability of the Air Force and the Army to train personnel for UAS operations,” and that “GAO found that the limited amount of DOD-managed airspace adversely affected the amount of training that personnel conducted to prepare for deployments. As UAS are fielded in greater numbers, DOD will require access to more airspace for training; for example, DOD estimated that based on planned UAS inventories in fiscal year 2013, the military services will require more than 1 million flight hours to train UAS personnel within the United States.”

“Further,” GAO pointed out, “Air Force UAS personnel and Army ground units have limited opportunities to train together in a joint environment, and they have not maximized the use of available assets during training. Current UAS simulators also have limited capabilities to enhance training. DOD has commenced initiatives to address training challenges, but it has not developed a results-oriented strategy to prioritize and synchronize these efforts. Absent a strategy, DOD will not have a sound basis for prioritizing resources, and it cannot be assured that the initiatives will address limitations in Air Force and Army training approaches.

In many cases, DOD’s UAS publications articulating doctrine and tactics, techniques, and procedures did not include updated information needed by manned and unmanned aircraft operators, military planners, and ground units to understand current practices and capabilities. Such information can serve as the foundation for effective joint training programs and can assist military personnel in integrating UAS on the battlefield.”

D’Agostino informed Congress last month that “DOD began plans for its Distributed Common Ground/Surface System (DCGS), an interoperable family of systems that will enable users to access shared ISR information in 1998,” but “DOD subsequently directed the military services to transition their service-unique intelligence data processing systems into DCGS and each of the military services is at a different stage.”
Heithold told Defense Systems that “we’ve done a very good job increasing our capabilities within the DCGS, not only technically with improvements we’re making within the weapons systems itself but also with the manning of the weapons systems. We’re doing a good job of using our total force initiatives to include the Guard and Reserve components. Today, the Guard actually is processing and exploiting 11 of [the] FMV combat air patrols that we have out there. This is in addition to the requirements that remain on the DCGS to [process, exploit, disseminate] and analyze intelligence from the various platforms that fly missions daily in the Central Command area of responsibility.”

“While the Air Force and the Navy each plan to have a fully functional version of DCGS by the end of fiscal years 2010 and 2013, respectively, the Army does not expect to have a fully functional system until 2016,” D’Agostino said, adding that “the Marine Corps has not yet established a completion date for the full operational capability of its DCGS.”

“To facilitate the sharing of ISR data on this system,” D’Agostino explained, “DOD developed the DCGS Integration Backbone, which provides common information standards and protocols. Although the services are responsible for managing their DCGS programs and conforming to information-sharing standards, according to the Office of the Under Secretary of Defense for Intelligence and military service officials, 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.”

And “without this overarching guidance,” D’Agostino cautioned, “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. Moreover, the inability of users to fully access existing information contributes to the increasing demand for additional ISR collection assets.”

Meanwhile, though, “from the ISR perspective, the need is just for more,” Air Force Maj. Gen. Tom Andersen, Air Combat Command’s director of requirements, told Aviation Week earlier this month.

And as new Al Qaeda franchises – the AQAMs – emerge and expand within their regional hubs of operation, IMINT will become increasingly important for identifying, tracking and, ultimately, disrupting them, counterterrorism authorities agreed.

“We have to be ready,” one said.