

Standardizing Infrastructure Patrols

The Maryland State Police Aviation Command, which regularly inspects important structures such as bridges, dams and power facilities, has helped to develop computer software that will assist all units in performing homeland security missions.

**By Sergeant Don Teesdale
Pilot/Homeland Security Liaison, Maryland State Police Aviation Command**

In a typical mission profile for the Maryland State Police Aviation Command (MDSPAC), any one of the department's 12 Dauphin helicopters will respond from one of eight strategically located helicopter sections to transport a critically injured patient to a trauma center, support police operations on the ground, or conduct search and rescue operations. Thousands of these missions are conducted every year throughout Maryland, as well as up to 30 miles into neighboring states when requested.

Since 9/11, a fourth mission category has been under constant development in the MDSPAC, the airborne critical infrastructure patrol (ACIP). The department is not alone, as many other state, local and federal aviation units conduct critical infrastructure patrols.

If your police aviation unit conducts patrols of critical infrastructure, you are indeed providing a critical service not only in your local jurisdiction, but also for your entire nation. Given the increasing number of law enforcement aviation units and their 24/7 operations, there is great potential for police aircraft to support an early detection, warning and response network throughout the nation. With the right tools, police aircraft can contribute to the common operational picture directly from "cockpit to patrol car," as well as to command centers at local, state and federal levels.

One of the exciting possibilities, though not without technical hurdles, is the use of wireless communications to send imagery direct from a laptop in the cockpit to a network on the ground. Public safety tools such as the Capital Wireless Information Network and Web Emergency Operations Center provide simultaneous information sharing across the strategic, operational and tactical continuum. If tools like these were accessible in flight they would dramatically improve on-scene communications and coordination. For example, an officer could use his/her patrol car laptop to highlight direction of travel and last known location of a suspect while the supporting aircrew shares the same map view.

Unless responding to a specific threat, MDSPAC helicopters conduct coincidental patrols during return legs from other missions. This is value added with little increase in operational cost. MDSPAC considers its fixed-wing resources to be ideally suited for deliberate patrols, launched specifically for ACIP using linear or route reconnaissance methods. An airplane can efficiently fill those reconnaissance gaps the helicopters miss and cover wider areas at lower cost. Since the early stages of this program, MDSPAC worked with key stakeholders in critical infrastructure protection (CIP), including the Maryland Emergency Management Agency and Maryland Coordination and Analysis Center, to select critical infrastructure and key resource (CI/KR) locations that should be patrolled.

The Towson Center for Geographic Information Systems (GIS), with development of the Maryland Emergency Management Mapping Application and the Maryland Emergency Geographic Information Network, helped us to better understand GIS standards (i.e. OpenGIS) and how mapping visualization could support information sharing between agencies. With respect to criminal data and information processing, we looked at the Regional Information Sharing System - Anti Terrorism Information Exchange and reviewed 28 CFR Part 23 relevant to the storage of criminal information on federally funded systems.

Compliance with this law was simple in our case, as we weren't looking to build another criminal database, but rather a critical infrastructure protection system.

We reviewed the Protected Critical Infrastructure Information Program to determine how it can help secure federal CIP data and strengthen public-private relationships. Private industries that partner with government must be assured that their vulnerabilities are not being disclosed or used against them. Public domain entities run as a business, so the bottom line financial situation is as much a consideration as the universal adversary. Police patrol is a security deliverable which protects the general public, not a process that constrains industry in red tape. Therefore, this was viewed as a "win-win" proposition.

Numerous vulnerability assessment methods were already under development. Among these are the automated critical assets management system, risk analysis and management of critical assets protection, and critical asset and portfolio risk assessment tool. We didn't need to reinvent the analysis wheel, but focused on turning vulnerability assessments into actionable patrol plans for police aviation and how to provide live feedback for those assessments.

The clearest way ahead is for police aviation to support a common operating picture with aerial sensors (infrared, video, thermal imaging, etc.) but there are needs beyond video downlink. Consider the entire information cycle (direction, collection, analysis and dissemination). Police aviation can support all of these components while serving as a defensive linebacker for buffer zone protection plans, defense in depth or similar strategies.

We soon realized the need for a comprehensive patrol system, including the people, processes and technology to support our critical infrastructure protection partners and stakeholders. A successful system would take an all-hazards approach to mitigate the actions of the universal adversary, whether natural or man-made. The system needed to be implemented on an enterprise level for the entire police aviation community and beyond.

We studied the strategies of our federal, state and private partners then looked at best practices in communities such as intelligence, surveillance and reconnaissance and aviation mission planning (i.e., FalconView and other GIS solutions). While military applications such as the Air Tasking Order provided possible solutions, their cost, accessibility or specific military nature made them inappropriate for police aviation needs. Military models led to development of other ideas, and the project underwent progressive elaboration.

After a period of information gathering, organizing our facts and assumptions and assessing existing capabilities and operational needs, we approached the Johns Hopkins University Applied Physics Lab (JHUAPL) with a request for technology assistance to build a GIS solution for the ACIP mission. The U.S. Department of Homeland Security Science and Technology (DHS S & T) Directorate's Command, Control and Interoperability Division recognized the nationwide potential for this proposed system and now provides support through program funding and strategic guidance for the project that we call the Critical Infrastructure Inspection Management System (CIIMS).

CIIMS (pronounced "sims") allows aircrew to select CI/KR sites while in flight using a tablet PC. The crew navigates to the sites using the software, which is linked by bluetooth to an automatic dependent surveillance broadcast, a small lanyard GPS or other NMEA 0183 standard geospatial data feed. Upon arrival at the site (within observable distance), the aircrew answers site-specific questions from the database then continue on it's way (e.g. Is the south gate secure? Are there any vehicles in the depicted area?). Upon return to home base, the tablet PC is synchronized over a secure network to upload data for further analysis and management of the patrol process.

Through the CIIMS database graphic user interface, authorized personnel upload site information for the patrols. "By-sector" reporting will enable feedback to those CI/KR sector specific agencies, information sharing and analysis centers or installations that request patrols of specific sites or otherwise participate in the process. This system can build on community oriented policing principles to enhance public-private partnership in the CIP community.

CIIMS has notably avoided proprietary modeling and stove piping, yet it is positioned to enable information led policing without information overload in the cockpit. Very few crewmembers have time to read "pass-through" reports or daily emails about threat incidents prior to flight, but they learn through crew resource management training how to ask for information when necessary. The key is to provide information to the aircrew in a manageable geospatial format.

Flight management considerations include frequency of patrol checks on sites and prioritization according to risk, consequence or threat. While algorithms may help prioritize the sites during lower threat levels, once actionable information is received, the system requires the ability to push mission tasks to

aircraft while in actual flight. The intelligence, surveillance and reconnaissance community would refer to this as a dynamic re-tasking capability.

A buzz term in the national security community over the past few years is "persistent surveillance", a concept that provides the enemy no ability to hide once detected. Queuing from one collection system to the next provides constant coverage until apprehension or other desired outcome is achieved. In development of such a concept, the police aviation community should not be overlooked, especially as the concept touches critical infrastructure protection. Certain mission tasking systems should be adaptable between military and law enforcement.

Although not directly connected to military communication systems, police aviation units are on the 24/7 front line of homeland security. Police aircraft are not only force multipliers, but also critical providers of detection, deterrence, interdiction, apprehension and response. Coordination with our military partners is vital, and differing roles under homeland security vs. homeland defense must be fully understood.

Infrastructure patrols should be properly coordinated between military assets and the 24/7 responders in the police aviation community for optimal resource allocation and appropriate jurisdiction. The incident command system presents an appropriate coordination platform for this.

CIIMS will eventually enter a commercialization stage, which will allow integration with flight mission computers, avionics, sensors or other GIS solutions. In addition, ground-based CIIMS applications are also undergoing research and the project partnership is beginning to expand.

MDSPAC personnel have been very excited about CIIMS. One of the key reasons for the success of the project is that Department of Homeland Security Science & Technology (DHS S&T) has continually ensured the entire CIIMS project is end-user driven by police aircrew personnel from project initiation to planning and execution. Strategic guidance and support from DHS S&T, as well as the excellent project management and engineering capabilities of our partners at JHUAPL have resulted in a very successful project.

CIIMS is rapidly growing into a tool that will support the simultaneous information sharing between strategic, operational and tactical levels of incident command. It is our vision that in the near future it will be a key component of information support to all law enforcement aviation units.