



11/13/06

Policing terror

Pioneering law enforcement agencies use data sharing and analysis tools to step up anti-terrorism contributions

BY John Moore
Published on Nov. 13, 2006

Thinking of local police as first responders recognizes only one of the important contributions they can make to homeland security. A recent Rand report suggests that local law enforcement is the critical line of defense for thwarting homegrown terrorist activity.

The book, "Unconquerable Nation: Knowing our Enemies, Strengthening Ourselves," states that the country's 600,000 police officers "are in the best position to monitor potential...terrorists."

Excerpt from Policing Terror

Teaming for intelligence

A New Jersey company and a software firm based in Israel are collaborating on an information-sharing and intelligence analysis system for law enforcement agencies.

Enforsys, a developer of public safety software, based in Roseland, N.J., teams with Svivot, a data analysis software provider with headquarters in Netanya, Israel. The companies received a grant from the U.S.-Israel Binational Industrial Research and Development (BIRD) foundation to pursue the joint development project.

The foundation matches American and Israeli companies involved in R&D and provides "funding covering up to 50 percent of project development and product commercialization costs," according to BIRD's Web site.

The Enforsys/Svivot project focuses on analysis.

"People are very focused right now on how [to] get the information shared and not asking enough about what to do with it," said Sam Roth, a Svivot executive vice president based in Boston.

Roth said the co-development effort aims to push data analysis beyond data mining. The goal is to move a step further into “inferring relationships among people and events,” Roth said.

The project involves integrating Svivot’s SN-Sphere software with Enforsys’ I-3 Exchange product for sharing incident-based and intelligence information.

Enforsys anticipates adding the Svivot intelligence functionality, SN-Sphere, in the first quarter of 2007, said Bill Plate, vice president of Enforsys. Previously deployed I-3 Exchange customers, which include Middlesex County, N.J., will also be able to add that functionality.

[Continue to read article in its entirety](#)

Rand says police can take advantage of their local knowledge to identify recruiting hot spots and develop intelligence sources.

But there’s a rub. Police departments require resources and training to pursue the intelligence dimension.

As a step in that direction, local and state authorities are starting to create intelligence centers that use information technology systems to gather, analyze and share intelligence data. Behind the scenes, technologists must gather multiple databases, engineer a fast and intuitive search capability, and provide a means to distribute alerts.

The integration task involves policy hurdles and technical challenges. Various jurisdictions must forge agreements to permit data sharing. In addition, law enforcement must follow state and federal data privacy directives.

Police agencies and their technology vendors take different approaches when it comes to intelligence analysis systems. Intelligence centers in Los Angeles and Louisiana are case studies of how such centers work.

Los Angeles’ take on intelligence

The Los Angeles Joint Regional Intelligence Center, dubbed JRIC, is one of the newest law enforcement intelligence centers. JRIC started in July as a cooperative effort involving the Los Angeles County Sheriff’s Department, the Los Angeles Police Department, the FBI and the Homeland Security Department.

JRIC’s local, state and federal intelligence analysts and investigators cover a seven-country region that encompasses more than 40,000 square miles.

The analysts use an intelligence management and analysis system from Memex, a company based in Glasgow, Scotland. The system lets analysts gather and track leads and collect information from various law enforcement data sources.

“Technical requirements were a system that was user-friendly, could manage cases for us, and do analysis on information contained in several data sources,” said Lt. Robert Fox, co-director of JRIC and the senior LAPD officer on site.

The latter system function — accessing multiple datasets — can present a technical headache. The scalability of a solution becomes an issue when organizations reach out to additional information sources, industry executives said.

JRIC's workaround is to replicate databases of interest inside the facility. Fox said the center draws data from traditional law enforcement systems but added that he couldn't identify specific databases for security reasons.

John McCarthy, director of law enforcement solutions at Memex, said the center replicates fewer than 10 databases. He added that it is negotiating to obtain additional data sources.

The center's schedule for replicating particular databases depends on factors such as the volume and volatility of the source data, with the frequency ranging from near-real-time to weekly.

The databases feed into a central repository, the Memex Intelligence Engine database. JRIC uses tools such as the Memex Extensible Markup Language Data Loader to migrate data.

In addition, JRIC programmers use application programming interfaces to build techniques for loading various databases, a Memex spokesman said.

Database integration raises policy considerations. For example, one part of the Code of Federal Regulations establishes data management and control guidelines for criminal intelligence systems receiving federal funds.

"To accept a copy of any organization's criminal database that has been funded by the federal government, you must agree to the same rules and guidelines that the parent organization has instituted," said Mario Cruz, IT project manager at JRIC.

Cruz said compliance tasks duplicate efforts and require an enormous amount of work to manage and monitor daily activity against the data.

But Cruz said that if organizations establish a memorandum of understanding with data sharing in mind, they can move data from one database to another without worrying about someone else's data warehouse policies. Databases can also be replicated within an individual agency without restriction.

As for future moves, JRIC will use the Global Justice XML protocol to connect to several federal databases.

In addition to structured data from databases, JRIC's data repository can also accept unstructured text data. People can drop electronic documents into Memex and scan paper records, too.

With the data in place, analysts can start combing for clues. Fox cited the ability to perform one-stop, drill-down searches as a major requirement.

Multiple searches on multiple data sources can take hours. In one test, JRIC found that the process of searching through 20 million records to isolate a phone number took 19 seconds with the new Memex system, compared with more than three hours using an older system.

In addition, McCarthy said the Memex analysis module can discover relationships among people, places and organizations that would otherwise remain unnoticed. Memex uses a proximity search capability to scour the intelligence database for those connections.

JRIC analysts share their findings with law enforcement agencies and other relevant parties through analysis reports, requests for information and e-mail distribution, Fox said.

Data fusion in Louisiana

The Louisiana Fusion and Analytical Center and Los Angeles' JRIC have similar goals, but the center has taken a different technical approach.

The Louisiana State Police launched the center for counterterrorism and crime investigation purposes. Apogen Technologies' Apogen Services subsidiary won a contract in July 2005 to develop the center's IT core.

That component involves a combination of custom and commercial products. On the custom side, Apogen has developed an incident reporting system based on Microsoft's .NET, said Scott McCumsey, Apogen program manager for the fusion center project.

The system, which runs on a SQL Server database, captures incident information from police who contact the Fusion Center. The system can also pull in reports of suspicious activity that people submit through the Louisiana State Police Web site.

By using the incident information, state police officers in the center can review leads and assign them to investigators. As a case unfolds, an automated workflow script routes incident information to the appropriate officers. The incident reporting system was moving into a beta testing phase at press time.

Another Fusion Center component lets analysts perform single searches of multiple data sources. The Louisiana Fusion Center's access extends to six Department of Public Safety databases. Those sources provide data such as criminal history, driver's license photos, driver's license images, driver's license/identification card information, motor vehicle registration and official driving records.

Analysts enter information such as name, sex and date of birth, and the system searches the databases and returns results based on that criteria, McCumsey said.

Instaknow, an Apogen partner on the fusion center project, provides the data integration software behind the single-search capability. Instaknow's approach doesn't require database replication.

Instead, the company's product emulates a user's access into each system. The software learns how an authorized person uses a Web browser to connect to an Internet or intranet database.

"You don't need a technical interface, nor do you need to copy [other parties'] data to your database," said Paul Khandekar, chief executive officer of Instaknow. "All we need to do is provide valid user IDs and passwords to Instaknow to access each of the source systems."

To share the data it collects, the center may make use of the Global Justice XML format. "Our intent is to be able to take information in the incident reporting system and use Global Justice XML to tag that information and make it available to other agencies through Web services," McCumsey said.

The fusion center also dispatches alerts based on its intelligence findings. Khandekar said center employees define the thresholds that trigger an alert — such as the number of felonies found for a person — and to whom the center should send alerts. Those polices are stored in a spreadsheet.

Epilogue

The IT deployments represent only part of the law enforcement intelligence-gathering picture. Law enforcement organizations must address cultural, policy and human resources issues to make a system work, industry executives said.

On the cultural side, organizations must be encouraged to share data. "The stumbling blocks to these initiatives are, generally, that people don't want to share their information, even if it's mandated," said Sam Roth, an executive vice president at Svivot, an Israeli firm that makes intelligence analysis systems for law enforcement agencies.

Police chiefs, he said, might balk at providing data if they think they are contributing data and not getting anything valuable in return.

Ronald Dick, director of homeland security, national security and foreign affairs at Computer Sciences Corp., said huge policy and legal issues face law enforcement organizations planning to share data.

He cited the case of "Sunshine Laws," which allow people to access information on state databases. Under those laws, an exemption restricts public access to information in the law enforcement category, he said.

But the situation becomes complicated if one agency shares data with another that can't protect the data under a law enforcement exemption.

Law enforcement entities also face security questions, such as whether employees have the authority to take classified information out of a federal system, said Morgan Wright, global industry solutions manager of public safety and homeland security at Cisco Systems.

Finally, the technology tools established to share and analyze data must have trained users at the controls, executives said.

The training component involves how to use the tools and being able to analyze the data that the various systems and databases provide, Dick said.

“It’s not entirely an IT solution and tools that are going to connect the dots,” he said.

Teaming for intelligence

A New Jersey company and a software firm based in Israel are collaborating on an information-sharing and intelligence analysis system for law enforcement agencies.

Enforsys, a developer of public safety software, based in Roseland, N.J., teams with Svivot, a data analysis software provider with headquarters in Netanya, Israel. The companies received a grant from the U.S.-Israel Binational Industrial Research and Development (BIRD) foundation to pursue the joint development project.

The foundation matches American and Israeli companies involved in R&D and provides “funding covering up to 50 percent of project development and product commercialization costs,” according to BIRD’s Web site.

The Enforsys/Svivot project focuses on analysis.

“People are very focused right now on how [to] get the information shared and not asking enough about what to do with it,” said Sam Roth, a Svivot executive vice president based in Boston.

Roth said the co-development effort aims to push data analysis beyond data mining. The goal is to move a step further into “inferring relationships among people and events,” Roth said.

The project involves integrating Svivot’s SN-Sphere software with Enforsys’ I-3 Exchange product for sharing incident-based and intelligence information.

Enforsys anticipates adding the Svivot intelligence functionality, SN-Sphere, in the first quarter of 2007, said Bill Plate, vice president of Enforsys. Previously deployed I-3 Exchange customers, which include Middlesex County, N.J., will also be able to add that functionality.

A sampling of intelligence sharing/analysis projects

Jurisdiction: Los Angeles and surrounding counties

Name of facility/system: Joint Regional Intelligence Center.

Mission: To share intelligence information among federal, state and local law enforcement agencies.

Type of technology: Intelligence management and analysis system from Memex. It uses database replication and can analyze structured and unstructured data.

Approximate cost: \$6 million.

Jurisdiction: Louisiana

Name of facility/system: Louisiana Fusion and Analytical Center.

Mission: To be a focal point for information processing, analysis and intelligence

production, using data collected by and shared among cooperating state and local agencies.

Type of technology: Custom incident reporting system, data integration and single-search capability via Instaknow, and Microsoft SharePoint-based Homeland Security Information Network and Jabber for secure instant messaging.

Approximate cost: \$735,000 for the initial contract with funding via a Homeland Security Department block grant.

Jurisdiction: Seattle and surrounding area

Name of facility/system: Law Enforcement Information Exchange Northwest.

Mission: To harness collective investigation efforts to better identify and resolve criminal or terrorist activity.

Type of technology: Data warehouse containing information from participating state and local law enforcement agencies. Northrop Grumman is the contractor.

Approximate cost: \$1.25 million in initial funding.

Enlisting local law enforcement

Brian Michael Jenkins, senior adviser to Rand's president and founder of that company's terrorism research program, discusses why local law enforcement officers are especially valuable to counterterrorism efforts and what they need to do that job more effectively.

FCW: *Your recent book, "Unconquerable Nation," points to 600,000 law enforcement officers as a key resource for combating homegrown terrorism. You talk about improving the intelligence capabilities of local police.*

JENKINS: The evolution of the threat demands that we enhance intelligence capabilities at the local level. As a consequence of the tremendous pressure put on the jihadist enterprise by the intelligence services and law enforcement agencies around the world, the jihadist enterprise has become far more decentralized. Self-radicalization takes place at the local level. Operations are planned and prepared at local initiative. And they are carried out with local content. We cannot depend entirely on the national intelligence services. We have to have greater local capabilities.

FCW: *Where should we see these enhanced capabilities?*

JENKINS: The threat is not the same in D.C. as in Duluth. So I think what we really are talking about is the major metropolitan areas that have the larger police departments and also happen to be very target-rich environments.

This is not to say that something might not happen in some rural community. The London bombings were planned in Leeds, a small city more than 100 miles from London. In our own experience, the Oklahoma City bombing was planned in various rural parts of the country. But I think the immediate challenge is developing these intelligence capabilities in the larger metropolitan police departments.

FCW: *So the local police are in a better position to pick up on things.*

JENKINS: These local terrorist operations are often financed through ordinary crime. Through routine criminal investigations, community policing or intelligence operations, the local police could be the first ones to pick up clues to a terrorist plot. If they — to use

the now-notorious phrase — connect the dots, that may enable us to prevent some of these future attacks.

FCW: *What types of resources do local police need as they take on this intelligence-gathering and analysis role?*

JENKINS: They need training. This is an intense human activity. They also need to have some means through which they can be wired vertically and laterally to be able to swiftly move information across jurisdictional and territorial boundaries. The New York Police Department has expanded its own intelligence operations and developed contacts with other police departments in the U.S. and abroad. In Los Angeles, the Terrorism Early Warning Group and the [Joint Regional Intelligence Center] address that problem at the local level, bringing together local police departments with state and federal entities.

At the national level, we have the Joint Terrorism Task Force, but that is a hub-and-spoke system. In an ideal world, we would have a communication system that respects the sensitivity of the information and, at the same time, allows a great deal of flexibility for autonomous entities within the network to organize around specific issues as information takes new directions or as new problems arise.

If you go back to the origin of the Internet itself, ARPANET was created to allow this free exchange of information among those involved in defense-related research. I'm saying we can create within the Internet something like the original ARPANET that will have the same flexibility for law enforcement.

FCW: *To go back to training, what are the issues there? Isn't counterterrorism a departure from the typical case-building work?*

JENKINS: Law enforcement is traditionally reactive. A crime occurs and law enforcement intervenes, gathers evidence, identifies and apprehends the perpetrator, and brings that person to justice. In today's world, where terrorists clearly are determined to carry out large-scale violence, a traditional law enforcement approach is risky. There is pressure on authorities to intervene early to prevent attacks. That depends on intelligence, not case building.