

Intelligence-Led Policing Evolves

Gartner RAS Core Research Note G00206971, Jeff Vining, 21 October 2010

The goal of intelligence-led policing is to anticipate and prevent crime and terrorism. A variety of approaches can be deployed to support this goal.

Key Findings

- Law enforcement agencies are challenged by how best to exploit behavioral and crime analysis of violent activity, with all the data being collected on a daily basis.
- Law enforcement agencies collect a lot of data through their computer-aided dispatch and records management systems. Historically, these systems have recorded crime and ensure quality of service, but have been of little use in crime analysis or prevention.
- IT managers must support all phases of intelligence-led policing processes and should consult the National Criminal Intelligence Sharing Plan (NCISP).

Recommendations

- IT managers should adopt the six steps from the NCISP for intelligence-led policing workflows and processes.
- IT managers should look at data already available and consider how to extract more value from it. Utilize tools to discover new patterns or confirm suspected patterns or trends to discern information that no one knew previously.

ANALYSIS

Background

Crime is often said to be unpredictable. To some extent, it is; but to some extent, it is not. While it is not possible to know exactly the location and time of a crime, using crime mapping and crime analysis tools, many agencies can now direct resources to so-called “hot spots.” This is in essence the definition of intelligence-led policing, which offers the capacity to provide decision makers with an operational picture of their environment (see Note 1). Intelligence-led policing strategies follow plans, such as the National Criminal Intelligence Sharing Plan (NCISP; www.it.ojp.gov/documents/National_Criminal_Intelligence_Sharing_Plan.pdf), which outlines a series of consecutive steps necessary to take to improve intelligence gathering and analysis. NCISP consists of the following six steps (see Figure 1):

- Planning
- Collection Process
- Collation
- Analysis
- Dissemination
- Re-evaluation

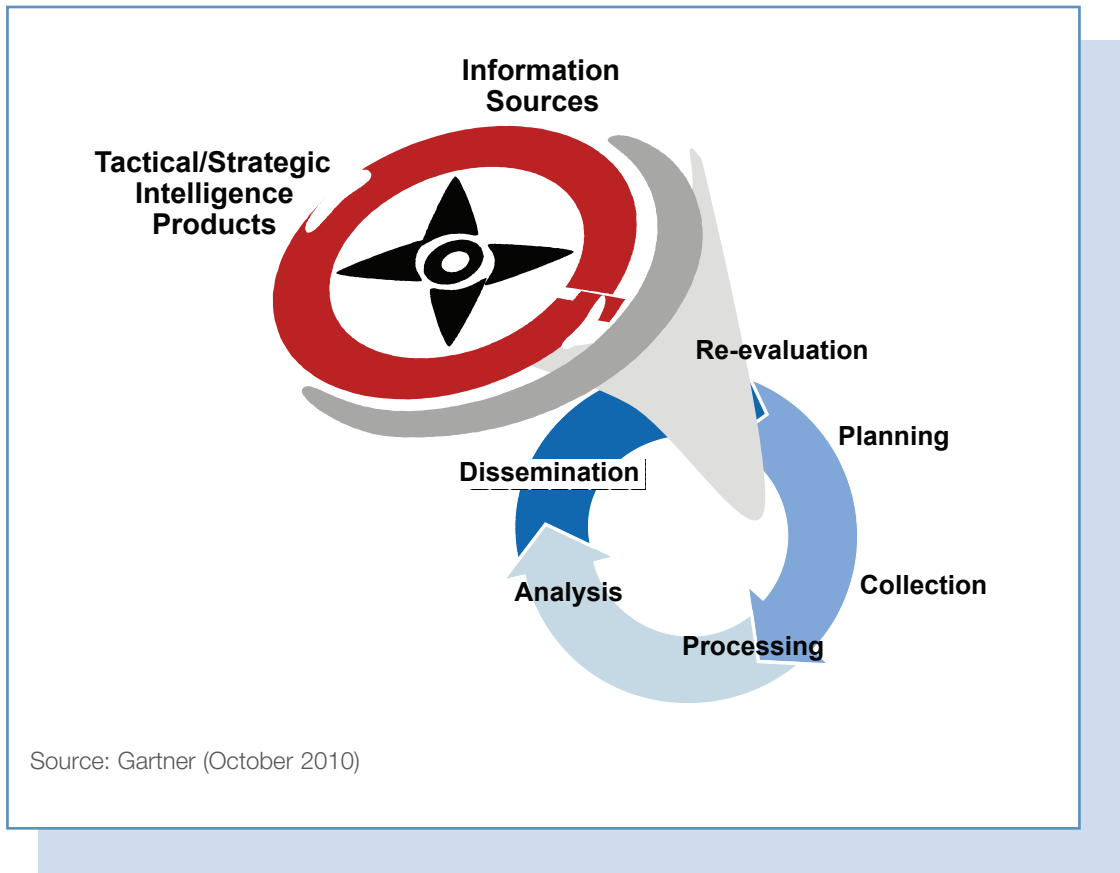
IT must support all phases of the intelligence-led policing process; however, through conversations with various clients, we find that some agencies primarily focus on Steps 3 and 4 and fail to address other areas. Reasons offered are agency culture, proprietary

systems, multiple data-entry points, lack of integration or poor data quality. Another factor, particularly within the U.S. state and local law enforcement realm, is budgetary. With many state and local budgets allocating more than 65% toward personnel costs, coupled with recent reductions of about 10%, the ability for IT to support its law enforcement agency is reduced further. With decreasing fiscal resources, IT managers are increasingly being asked to do more with less. Gartner examines five of the six steps under NCISP and offers some agency-specific examples that have evolved under these conditions.

Planning

Just because an agency has data and analytical tools does not mean it will have an effective intelligence-led policing strategy. IT managers must first understand the challenges (types of crimes, available resources, demographics and geography) to overcome. Law enforcement agencies deploy two basic types of field units: patrol and tactical for crime interdiction and prevention.

Figure 1. Intelligence-Led Policing Process



To better allocate these resources, units divide themselves into geographic precincts that are further subdivided into sectors. Tactical is responsible for a given sector but often lacks sufficient insight about deployment, which results in skill underuse and an overdependence on patrol for crime interdiction and prevention. IT managers formulate questions about operational environments to better define priorities for data collection and intelligence analysis to better support deployments, such as:

- How can I provide an accurate snapshot of activity in real time?
- How can I better define the types of crimes and associated social and environmental factors?
- How can I monitor trends and prioritize between threat levels?

Next, blend intelligence information (criminal investigations in support of specific crimes) as well as more dedicated intelligence information (drug trafficking, financial crimes, terrorism-related crimes) with specific department objectives such as reassign patrol units or reduce felony crimes by 25%. This requires IT managers to match identities and relationships by linking disparate data elements on people from information sources. This requires assessing how to extract key criteria (people, address, vehicles, weapons and phone numbers) to compile a matrix that lists types of information to be collected from types of sources (logical, physical and social).

Collection

This is the phase where consumers at all levels must define their priorities, for source information for IT managers is beset by large quantities of information, and data collection is a labor-intensive process. IT managers use systems to feed data warehouses through an extract, transform and load data pipeline, then apply analytics using business rules to discern patterns. Gartner is informed that many state and local government agencies downselect as follows:

- Open-source information types: Internet sources, public records, business directories
- Government sources: computer-aided-dispatch (CAD) systems, records management systems (RMSs), video surveillance images, electronic surveillance, financial institutions, law enforcement databases and confidential informants

A challenge is defining if source types and data are valid – not irrelevant or incorrect. This requires a formalized entity resolution and analysis process based on techniques used in data integration and master data management. However, this is time-consuming and resource-intensive. IT managers are looking for alternatives to use existing data and to consider how to extract more value from it.

Example: One approach comes from Virginia, where five different Virginia jurisdictions have formed the Roanoke Area Criminal Justice Information Network (RACJIN), linking multiple CAD/RMS databases using Memex software (a SAS company) and other third-party software tools to search for and analyze criminal information. From an intelligence-led policing perspective, it quickly raises the number of searchable records for an identifiable suspect, but the approach is not focused on eliminating invalid CAD data.

Collation

This step requires the sifting of data sources to eliminate invalid data. If this process is successful, valid data is used to determine event and pattern sequences. Many law enforcement agencies use content analytic applications to process text, graphics, multimedia, audio/video and other unstructured data. The main drawback to this approach is that many content-analytic applications can only process one data type. For instance, for text, many agencies will use IxReveal-type applications and remain focused on applications. As a result, agencies lack vision. IT managers should think about other types of complementary data.

Example: The Richmond, Virginia, Police Department uses data mining, interactive visualization, public source data and other unstructured information for its intelligence-led policing strategy. Data is collated into predictive geospatial models that are built into dashboards to gain insight into specific crimes, with data being collected and collated through the police department's 911 system, using CAD/RMS. This is integrated (using Information Builders' WebFOCUS Web interface) with the Richmond.com website to add information about local activities and weather likely to affect crime. Results are displayed with aerial photography from Pictometry and ESRI maps and SPSS's PASW Modeler data-mining tools.

Analysis

Analysis translates data based on evaluation from multiple sources to derive meaning. Intelligence-led policing should be integrated into existing processes because, unlike retail analysis where predictive variables (customer and demographic information) are not likely to rapidly change, crimes (suspects being identified and apprehended) change rapidly. IT managers must explore factors, such as time of day, day of week and geography associated with specific crimes (such as robbery) to analyze and predict areas of future activity. Gartner has found that many IT managers are opting for business intelligence platforms offering easy-to-use interactive visualization technologies (Microsoft with PowerPivot, SAP with BusinessObjects Explorer, IBM with Cognos Express and Information Builders with WebFOCUS Visual Discovery) to estimate and classify criminal, environmental and societal variables. Gartner views this approach based on predictive analytical models and forecasting algorithms that can be consumed in reports and dashboards as viable, but cautions agencies that they may still find themselves "data rich but intelligence-led-policing challenged"; particularly when too much heterogeneous data is being consumed – much of it never being intended for analysis. For example, a 911 call in which multiple vehicles are dispatched with only one officer filing a report skews data on the actual vehicles dispatched.

Example: The analogy that a picture – or graphical representation – is worth 1,000 words is readily apparent when highlighting data on a map to enable users to easily see things that might be harder to understand on paper or more-static models. The New Jersey Regional Operations Intelligence Center (NJROIC) uses data mining, interactive visualization and other unstructured information to support intelligence operations for multiple agencies using SPADAC Signature Analyst tools to analyze various factors (time of day, day of week, location, modus operandi) to create geospatial models to predict likely criminal activity and probability of conditions for crime occurring (see Note 2). Demands for more-current data to prompt further exploration are allowed to challenge existing models. IT managers can also look at other vendors such as Sentient, SAS Institute, KXEN and SPSS for similar representations.

Dissemination

The majority of violent crimes are committed during evenings and on weekends when staffing is minimal. IT managers cannot wait for personnel to return to work. Given the sensitive nature of intelligence-led policing information, it is important to adhere to certain procedures with regard to information dissemination, which requires transferring actionable information to people who have the need and the right to use it. For example, the University of Miami police deploys electronic scripts produced using existing crime analysis tools and CAD event data, alerting officers while on patrol to move toward various locations where certain types of crimes are likely to occur.

Examples: The Commonwealth Fusion Center in Massachusetts needed to communicate and disseminate Intelligence-led policing information among and between multiple jurisdictions and agencies. It opted to deploy an ESRI ArcGIS Server and multiple specialized Microsoft SQL Server databases, linked via Microsoft Office SharePoint Server.

Note 1 History

The intelligence-led policing concept originated at the Kent Constabulary, United Kingdom, in response to increases in property-related offense. Kent de-emphasized responses to service calls by prioritizing calls and referring less serious calls for nonpolice services to other agencies. Thus, more police time was available for intelligence. This idea became the focus for the 2003 National Criminal Intelligence Sharing Plan. For more information, see www.ncjrs.gov. In essence, this model suggests that police view crime as a business and develop methods and deploy technologies to gain an accurate picture of the business (what is actually happening, trends in the business and how to neutralize threats). Other intelligence-led policing models have emerged such as scanning, analyzing, responding and assessing (SARA), sometimes referred to as problem-oriented policing.

Note 2 NJROIC

For more information, see “Geospatial Statistical Modeling for Intelligence-Led Policing,” *The Police Chief* (August 2010), pages 72-76; [www.nxtbook.com/nxtbooks/naylor/CPIM0810/index.php - /72-76](http://www.nxtbook.com/nxtbooks/naylor/CPIM0810/index.php-/72-76) (Raymond Guidetti, Lieutenant, New Jersey State Police; and James W. Morentz, Ph.D., Senior Homeland Security Advisor, SPADAC).