Geospatial Intelligence for Fusion Centers

Geospatial Intelligence for Fusion Centers

An Esri White Paper

Geospatial Intelligence for Fusion Centers

Executive Summary

The Department of Homeland Security (DHS) has published many documents defining fusion center best practices and processes, yet much still requires further discussion. The purpose of a state or local fusion center is to facilitate the collection, analysis, and dissemination of crime- and terrorism-related information. A fusion center is often defined as a collaborative effort of two or more agencies providing resources, expertise, and information. The goal is to optimize the ability to detect, prevent, investigate, and respond to criminal and terrorist activity.

Fusion center workflow and technology requirements are complex. The primary focus of a fusion center is to analyze suspicious activity reports (SARs) and crime to identify preoperational terrorist activity. The following are key workflow steps for a fusion center:

■ Intelligence collection
■ Data integration and fusion
■ Information analysis
■ Production
■ Knowledge dissemination

Many technologies and data sources are needed to support the fusion center mission. These include collaboration tools, network services, business logic software, workflow systems, and data analysis tools.

Geographic information system (GIS) technology fully supports the fusion center workflow, resulting in the ability to rapidly process and disseminate actionable knowledge, collect feedback, and quickly share updated information. This is accomplished by using a flexible exchange platform supporting interoperability with other systems. It relies on open standards that enhance situational awareness by fusing disparate information with its common reference—geography.

The purpose of this white paper is to discuss how GIS technology supports the fusion center intelligence cycle workflow.

Operational Objectives

Typically, fusion centers are staffed and operated by law enforcement agencies. Due to budget and policy issues, fusion centers are often taking on an expanded role by collaborating with multiple agencies such as emergency management and fire/rescue. Many fusion centers have Federal Bureau of Investigation agents and DHS counterterrorist analysts colocated to support information sharing.

There are three classifications to a fusion center's operational objectives:

- All crimes
- All risks
- All hazards

DHS has published guidelines that provide high-level requirements for establishing a fusion center. However, there is little documentation to clearly define fusion center technology capabilities. Many fusion centers often rely on consultants or their IT departments to determine what technology is required to support operational objectives, funding, and staffing.

All Crimes

With the growing expectation that fusion centers do more than focus on counterterrorism, many law enforcement agencies approach their intelligence capabilities from an "all crimes" perspective.

The all crimes approach can be defined as information pertaining to criminal behavior or man-made events. The intelligence analyst must sift through volumes of terrorist activity data while attempting to identify broad-based criminal patterns and behaviors. All crimes would include drug trafficking, organized crime, money laundering, illegal gang activity, and auto theft.

The data needs or requirements for the all crimes approach include crime records, computer-aided dispatch (CAD) system data, suspicious activity reports, investigative files, evidence data, court cases, and news reports. These datasets can be georeferenced and visualized on a map in terms of a single location point (dot) or concentrations and density polygons.

All Risks

The "all risks" approach examines the probability of a man-made or natural disaster occurring. For example, the likelihood of a hurricane causing damage in Las Vegas, Nevada, is remote. However, the likelihood of criminal intent to detonate a weapon in the middle of a crowded city area, such as Las Vegas, is much greater.

The fusion center analyst driven by an all risks approach would seek evidence and other data pertaining to threats determined to have a higher degree of possibility or probability of occurring. Risks are also about vulnerabilities such as where mitigation is the weakest and what has to be implemented to account for possible threats before they occur. GIS can help in assessing risks and identifying threats before they become a major concern.

All Hazards

The "all hazards" intelligence analysis approach includes crime, but the analyst also focuses on natural and technological hazards such as earthquakes, hurricanes, floods, and hazardous-material spills. This approach considers fixed locations of infrastructure, assets, and values and analyzes the types of hazards that could incapacitate them.

The fusion center chartered with an all hazards operation collaborates with multiple agencies including emergency management and fire/rescue. It supplies a comprehensive approach to sharing threat, risk, and values information to provide situational awareness for a more informed emergency planning, preparedness, response, and recovery effort.

Fusion Center Intelligence Cycle

While fusion centers may operate independently, they have common workflows and best practices. Every fusion center operates using four steps in the intelligence data cycle: collection, integration, analysis, and dissemination. Those four steps are continuous. They require feedback and input from external sources to create new data that is fed back into the cycle to validate and evaluate different intelligence variables.

GIS integrated within an IT enterprise supports the fusion center intelligence cycle in three key areas:

- Analysis and identification of data relationships
- Decision and workflow automation
- Visualization, production, and dissemination of data and information

Data fusion is essentially the process of collecting and integrating information from disparate sources to understand relationships and make discoveries. Many solutions in the market today provide that level of capability. However, the mission of a fusion center is more complex. It requires the ability to analyze and create information products such as an intelligence report or briefing. Perhaps most important, it also must be able to easily share information at local, state, national, and possibly international levels.

Several solutions provide the ability to do simple mapping, or provide dots on a map. GIS is the only technology that supplies true analysis and modeling power that fully integrates and supports existing information technology investments. It also provides true data integration and sharing. A common misconception is that visualizing dots on a map is a way of sharing data. Location mapping does not provide access to the data behind the location. Users can't consume data in existing workflows or apply analytic models to it. GIS supplies these capabilities. The fusion center analyst can access data related to map locations to more reliably identify patterns and trends. GIS provides the ability to gain an understanding of the relationships between all types of data, such as the location of a suspicious activity report vis-à-vis critical infrastructure.

Information Sources

All data and information can be organized using the location, alphabetical, time, category, and hierarchy (LATCH) method. Data can be organized by its reference to a place or location; in alphabetical order based on a key data field; by date and time; by category or the source of data; or by hierarchy, such as security classification levels or importance of the data. However, the lowest common denominator of all data is its reference to location. Information can be broken into three fundamental types for the purpose of fusion center functions: basemap, operational, and dynamic.

Basemap Data

Basemap data remains relatively consistent in location, characteristic, and situation and over time. Geospatial data representing jurisdictional and community boundaries, streets and transportation routes, and aerial or satellite imagery is essential for defining a basemap. In addition, some community characteristics—such as critical infrastructure, common places (schools, nursing homes, hospitals, banks, places of worship, restaurants, bars, train and bus stops, etc.), and economic data—can be included in a basemap. This provides fusion centers with an analytic reference. Basemap data essentially determines what has to be protected in terms of our environment and surroundings. Basemap data is essential in determining what has been or will be impacted by a threat or event.

There are many sources of basemap data, including state, county, and local governments and commercial references. Specifically, these can include Bing™ Maps, NAVTEQ® data provided through Homeland Security Infrastructure Program (HSIP), and Esri's ArcGIS.com.

Operational Data

Operational data is typically collected, analyzed, maintained, and disseminated during the fusion center intelligence cycle. Tips and leads are typical sources of operational data that a fusion center maintains. In addition, the fusion center often requires access to crime data stored in various law enforcement and fire department record management systems (RMSs). Law enforcement RMS data is historical information regarding crime activity in a community, while fire RMS data provides historical information pertaining to fire/rescue incidents.

When analyzed in conjunction with RMS data, tips and leads can be the determining factor in threat identification. For example, an investigation of a structure fire reveals that the fire started as a result of an illegal meth lab at the location. Since it is widely known that terrorist organizations fund their operations through criminal activity, the location of a suspected drug lab would be of interest in evaluating the potential of a larger threat.

Dynamic Data

Dynamic data is information that is changing in location, characteristic, or situation or over time, for example, resource/asset location tracking data. Live feeds from news and weather agencies, sensors, and video/multimedia and detection devices provide event data for creating situational awareness.

Geospatial Analysis of Data

To facilitate the analytic process, products that are consumer tailored, clear, and objective must be used. These tools support the development of performance-driven, risk-based prevention, protection, and response programs. Analytic capabilities are dependent on strong data collection, integration, and management practices as well as whether the fusion center operational objective is all crimes, all hazards, or all risks.

Some of the fusion center analytic products include

■ Link analysis: Associations between people and places

■ Threat identification: Confirmed SARs

■ Risk assessments: Areas vulnerable to threats such as critical infrastructure

■ Critical infrastructure protection assessments: Buffer zone protection planning

■ Requests for information validation: Disseminated briefings for detectives and investigators

■ Crime analysis reports: Areas where crimes are occurring

Creating those types of analytic products requires access to multiple data sources such as crime records, multimedia, sensors, suspicious activity reports, unstructured information, and incident data. GIS provides the ability to normalize this data plus much more, based on geography. In addition to normalizing capabilities, GIS provides the ability to model

and analyze data to determine spatial relationships, which are more visually intuitive than tabular data.

Crimes

Nearly every law enforcement agency in the United States maintains crime data in a record management system. The exception might be found in smaller jurisdictions, such as rural towns that may still keep paper rather than electronic records. The data is accurate and highly sensitive, as it contains information on suspected and convicted criminals and their crimes as well as investigative material used in prosecution.

Crimes have unique geographic characteristics dependent on many factors, including the concentration of gangs or known offenders. However, patterns, trends, causes, and relationships can be identified by analyzing their geographic reference. The output of the crime analysis can be a hot spot or density map that illustrates concentration of a particular type of crime or the aggregation of all crimes to determine high-risk areas.

Criminal activity can be an early indicator of terrorism threats within the community. It is widely known that terrorist organizations are particularly interested in engaging or recruiting people with a tendency to commit crimes, such as gangs or organized crime groups. These types of criminals may not even know they are aiding a terrorist organization plot. They typically are involved because of some sort of financial or influential gain. The types of crimes they typically commit can range from drug trafficking to more sophisticated activities such as money laundering. Detailed information contained in investigative reports can be used to link related crimes to one another, providing the ability to identify patterns. Evidence captured in the investigative reports can also supply leads to other crimes or activities. Sharing information on precursor crimes can often trigger a connection to similar incidents to potentially identify a larger threat. Geographically linking crimes to offender databases (corrections, jail, parolee, sex offender, most-wanted list, etc.) can lead to identifying relationships between the criminals and terrorist organizations.

For example, a crime analyst could use spatial analytic models to link a particular geographic area's increase in crime to a criminal who was just released on parole based on parole date, location, and prior behavior. Social link analysis in a geographic area and visualizing a parolee's behavior and relationships can help identify connections to larger organizations such as gangs or fundamentalist groups.

Suspicious Activity Reports

Suspicious activity reports can be early indicators of an imminent threat. The Department of Homeland Security has been designing a tool and standards for SARs to ensure that the data is shareable throughout agencies and fusion centers. SAR data should be geocoded to make it easier to search for reports proximal to an area of interest (e.g., incidents that have occurred close to critical infrastructure or SARs with similar characteristics).

For example, after being tasked to review a new SAR, a fusion center analyst can access a map to visualize the location of the suspicious activity. The analyst can then perform a proximity search for SARs with similar characteristics such as photography, observation, security testing, and type of vehicle involved. A proximity search will show whether there are other activities occurring in the same area over a period of time. Performing a proximity search will also show nearby critical infrastructure, planned special event locations, and populated areas.

911 Incident Data

A fusion center analyst can learn much from 911 incident data. Linking current and historical 911 data to SARs can provide insight into events that may be an early indication of a larger or imminent threat. An accurate location or address is a requirement for dispatching emergency resources. Most computer-aided dispatch systems include the location in every incident record, making the data an excellent fusion center resource that can be accessible through GIS. Collecting 911 data from multiple emergency dispatch centers can be quite a challenge due to disparate and proprietary data formats and systems. GIS can normalize 911 data based on its common reference geography.

For example, a fusion center receives an SAR of several men loading 55-gallon drums into an unmarked vehicle in the middle of the night. The vehicle's license plate number was also reported, and the address for the registered vehicle is on record. Days later in another community, a 911 call is received about a man having difficulty breathing. The address of the 911 call is the same as the address of the vehicle involved in the SAR. This scenario may have a legitimate explanation or be something more serious. The fusion center analyst can alert law enforcement and make a threat assessment based on this type of link analysis.

Open Source

The Internet is another source for intelligence data to be consumed and managed in a fusion center. Much of the content on the Internet is unstructured and open source. Therefore, the data needs validation. However, there are spatial tools that provide the capability of geocoding unstructured data over the web so that it can be visualized on a map. Open source data includes news reports, commercial products, website content, blogs, audio files, published documents, and RSS feeds.

For example, fusion center analysts using a map for situational awareness would have the ability to see when a news report appears on the map through a GeoRSS feed. Analysts can access and read the news report, which may have information that triggers a connection to an SAR they had been working on. The analysts can then query the map to locate the SAR and update their notes based on the news report details.

Conclusion

GIS supports fusion center workflows and provides interoperability with other systems. It improves collaboration and communication throughout the intelligence cycle. When integrated with workflow and web-based collaboration tools such as Microsoft® SharePoint®, GIS is a complete information management system, providing capabilities in the following environments:

Desktop

GIS desktop tools provide the ability to visualize patterns of suspicious activities and to model vulnerabilities. Threats to critical infrastructure, populations, and other community values are quickly identified with GIS, and spatial models can help analysts determine consequences. This type of work is typically performed by a GIS technician using the power of ArcGIS® Desktop technology.

Web

Fusion center analysts can publish their findings and work products through a web-based GIS common operating picture (COP). This improves collaboration and information sharing throughout the organization. Fusing base and dynamic data, such as weather, traffic cameras, video, GPS, 911 calls, and SARs, allows analysts to easily supply a complete picture. GIS integrates with collaborative technologies such as Microsoft SharePoint, providing a comprehensive information management workflow.

Mobile	Meeting mission demands often requires the ability to provide mobile workforce information in the field. Fusion centers frequently need to provide law enforcement and investigators with information related to suspicious activity, such as its proximity to critical infrastructure, related SARs, or other crimes. Law enforcement officers and investigators can have access to such details via a portable laptop, PDA, or mobile phone. They can also send field information back to command centers for true situational awareness.
Online Maps and Data	ArcGIS℠ Online and ArcGIS.com provide access to a library of GIS data, imagery, and other software applications. They are a key component of the ArcGIS system for emergency/disaster management. A variety of worldwide basemaps is available, including imagery, streets, topography, and community basemaps. Homeland security personnel can create private or public groups to exchange map data, projects, and presentations.
GIS Server	ArcGIS Server is the core component of GIS for fusion centers. It can be deployed within the fusion center or hosted in the cloud and provided as a GIS service. ArcGIS Server provides the platform for information analysis and management to perform threat detection and assessment. ArcGIS Server also provides mobile connections to consume updates and edits, which are stored in the database and published to the situational awareness viewer. It also enables access to dynamic data, services, and other online GIS data that is made available to all other GIS clients and viewers within the system.

About Esri

Since 1969, Esri has been helping organizations map and model our world. Esri's GIS software tools and methodologies enable these organizations to effectively analyze and manage their geographic information and make better decisions. They are supported by our experienced and knowledgeable staff and extensive network of business partners and international distributors.

A full-service GIS company, Esri supports the implementation of GIS technology on desktops, servers, online services, and mobile devices. These GIS solutions are flexible, customizable, and easy to use.

Our Focus

Esri software is used by hundreds of thousands of organizations that apply GIS to solve problems and make our world a better place to live. We pay close attention to our users to ensure they have the best tools possible to accomplish their missions. A comprehensive suite of training options offered worldwide helps our users fully leverage their GIS applications.

Esri is a socially conscious business, actively supporting organizations involved in education, conservation, sustainable development, and humanitarian affairs.

Contact Esri

1 800 GIS XPRT (1 800 447 9778)
T 909 793 2853
F 909 793 5953
info@esri.com
esri.com

Offices worldwide
esri.com/locations

380 New York Street
Redlands, California 92373-8100 USA