An ESRI® White Paper • May 2007

GIS Supporting the Homeland Security Mission

ESRI 380 New York St., Redlands, CA 92373-8100 USA
TEL 909-793-2853 • FAX 909-793-5953 • E-MAIL info@esri.com • WEB www.esri.com

GIS Supporting the Homeland Security Mission

An ESRI White Paper

Contents **Page**

GIS Supporting the Homeland Security Mission

Executive Summary

It is common knowledge that the Department of Homeland Security (DHS) was established as a federal department in direct response to the terrorist attacks that occurred on September 11, 2001. One of the intentions behind forming DHS was to provide greater security against additional threats through better coordination across multiple jurisdictions and agencies.

Since the formation of DHS, we have learned that security means more than protection from terrorism—it means protecting life, property, and critical infrastructure from any disaster (natural or man made). The events of Hurricane Katrina demonstrated how quickly our nation's infrastructure can become overwhelmed and/or disabled, leaving much in jeopardy.

As a nation, we continue to learn how technology can better enable government and public safety agencies to manage information in the mission of securing our homeland. The demand for authoritative data from various sources to create a common operational picture is found at all levels of government. Whether it is intelligence data on potential threats, analytical data for preplanning, or real-time data for emergency management, there must be a willingness to share data as well as the technical capability of providing it in a usable manner. However, data sharing comes with a cost and should be done with consideration to the sensitivity of the information. Some existing laws limit the type of information that can be exchanged in order to protect the civil rights of individuals and the business needs of industry. Strategic or classified information also requires a high degree of security.

Every event or situation is associated with a point on the earth. Understanding the interplay between these points can mean the difference in knowing whether the situation is localized or is something much bigger. Geographic information system (GIS) technology provides the capability to understand how events relate to each other and the impact they have on infrastructure and networks, making it a critical component of any homeland security or public safety IT infrastructure.

Introduction

This paper will illustrate how GIS can be applied as part of a comprehensive homeland security technology strategy. It is not intended to provide technical specifications or specific implementation recommendations but more a general perspective of technical considerations.

Since 2001, homeland security, as a practice, has been maturing and growing to meet the demands of protecting our nation from natural and man-made threats. Law enforcement agencies from all levels are actively gathering and analyzing intelligence data to qualify or devalue threat targets, and emergency response agencies are preparing and planning to prevent, or reduce the consequences of, another large-scale terrorist attack. Whether an event is a suspicious activity or an emergency incident, it takes place at a local level, and as more information is learned or the situation escalates in severity, information

management becomes more complex. The term *severity* is best defined as the scale at which an event impacts life, health, property, and the economy.

In a catastrophic situation, information management complexity is commensurate with increased need for system standards, business processes, agency relationships, and information technology requirements.

Homeland security involves many disciplines including law enforcement, intelligence, fire/rescue, health care, and critical infrastructure protection. No matter the discipline, any time the severity of a situation increases, there is an increased need for complex systems to manage the situation.

For example, a typical residential structure fire is severe by any standard, especially to the owner of the property. However, the complexity of information technology needed to respond to the fire may be as simple as knowing where the incident is and how to get there. Typically, first responders have little time to perform scene size-up and provide direction to the response team. A small incident is quickly contained and requires minimal information beyond what is available on the scene.

However, a fire that involves a commercial structure with hazardous materials inside dictates the need for additional information and requires better information technology systems. Incident commanders need to know much more about the situation than just its location. In a large event, an incident command post will be established involving multiple agencies. Obtaining and sharing information from various sources will be essential in ensuring the situation doesn't escalate any further.

If hazardous materials are released, incident commanders will need to know the impact weather has on the situation. Which way will a vapor cloud travel? Who in the community is most likely in the path of the vapor cloud? Who needs help evacuating, the elderly in senior centers or children in schools? Where can triage and decontamination sites be established? Where are the evacuation shelters? What are the most appropriate evacuation routes? What hospitals and trauma centers should prepare for inhalation victims?

Mutual aid responding from neighboring communities may also be affected by the same event. The incoming units, typically unfamiliar with the area, will need to know where to go and how to get there as well as how to avoid contamination.

Incident commanders will need to know when incoming units have arrived in staging as well as their functional capabilities. Law enforcement will require situational awareness to respond effectively. Public works and utilities will also need detailed information to protect and sustain critical infrastructure.

In the case of a large-scale event, such as a hurricane or a health pandemic, the complexities of resource coordination and information management increase dramatically. This will involve all levels of government and will require the integration of many information systems and agencies.

GIS provides decision makers with the spatial awareness to understand the overall impacts and potential exposures to surrounding areas and critical infrastructure so that resources can be deployed more effectively.

GIS in Homeland Security

To better describe how GIS is woven through the technology fabric of homeland security, this paper will examine six essential topics:

- Strategic planning
- Common operational picture
- Critical infrastructure protection
- Emergency Operations Centers
- Data fusion
- Response exercises

Strategic Planning

Preparedness is the greatest determining factor in the successful resolution of an incident or event. Therefore, strategic planning is essential for ensuring an effective response to homeland security threats.

Strategic planning is defined as the systematic identification of future opportunities, vulnerabilities, risks, and threats (both external and internal) that, in combination with other relevant data such as available resources and capabilities, provides a framework to make critical decisions in an emergency situation.

Strategic planning is a multidimensional process that involves intelligence gathering, risk assessment/analysis, response scenario modeling, and documenting procedures as well as training and practice.

The process of strategic planning begins with gathering and collecting data. Data identifies the who, what, when, and where variables in any potential event. Data can come from many sources including local records management system (RMS) repositories, state databases, and data collection projects seeking specific or specialized information. The important thing to ensure when gathering data is that it is spatially referenced or geocoded.

Spatial reference could be at any level from a precise GPS pinpoint to a general location such as a city boundary. In either case, the idea is to create a better understanding of the relationships between different data records through geocoding. Geocoded data is essential for geoprocessing or deriving information from two disparate datasets, which will be discussed later in this paper.

Geoprocessing is performed during the analysis and modeling phases of strategic planning. Geoprocessing is essentially the systematic work performed by GIS analytical tools such as ArcGIS® and identifies the impacts of an event on a particular community, neighborhood, or critical infrastructure. Models can be implemented, and various types of scenarios can be modeled by changing the variables. In this stage, data is visualized in the context of a map. By focusing on a particular risk, GIS analysts can create a scenario and visualize the potential effects on the community. The effects of a particular event may be reduced with the appropriate mitigation actions, which can also be identified and modeled.

The results from the modeling phase can be used to document agreed-upon prevention, interdiction, mitigation, and response requirements and training needs. Maps, building diagrams, and other preplan data could be used as illustrations within the written procedures, providing more effective communication, or for training exercises.

It is not enough to simply communicate response plans. They must also be practiced as part of an overall training program. This final stage is critical to ensure the strategic plans are effective as well as easily understood and implemented.

The use of GIS as an effective tool in the training process is discussed later in this section.

Common Operational Picture

In a crisis situation, the effort that ensures all individuals and teams involved in operations or command have the same information is commonly referred to as a common operational picture (COP). The intersection of strategic basemaps, critical infrastructure protection, intelligence data, and emergency operations in a defined taxonomy creates the information management construct for a COP.

Strategic map data is the foundation for operational situational awareness in a specific geographic area. The strategic map data consists of street centerlines, address information, common places or areas of interest, and critical asset locations. When basemap data is merged with operational data fed from active incidents, consequential data from critical infrastructure threat models, and data from intelligence fusion centers, a more comprehensive view of activities, threats, and situations is obtained for better and timelier decisions for terrorism prevention, interdiction, and/or response when required.

A common operational picture can be obtained through the use of multiple technologies and/or media synthesized on their common location element. It is important to equip a command center with as much connectivity to information sources as possible including live news feeds, weather data, live map data, remote-sensing data, tabular data, building plans, and charts/graphs. The end user then has the opportunity to "turn on" the data they need relevant to their mission to create actionable information.

Critical Infrastructure Protection

Hurricane Katrina in 2005 demonstrated the need to better understand how to protect our nation's infrastructure. The loss of communication, power and energy, water and water treatment, and food as well as medical supplies can make quality response and recovery very difficult and, in some cases, almost impossible. The long-term effects to the community and the economy are yet to be truly understood.

Critical infrastructure data collection projects have generated a significant amount of interest in using GIS technologies. GIS enables the ability to model events and geospatially determine risk potential and mitigation alternatives. For example, mapping the location of an electrical power grid in the event of an explosion or attack that has caused a loss of power could help emergency response planners know which parts of the community may require more help than others and where the system is most vulnerable. The information could also be used in planning the economic impact of a terrorist attack on the same power system.

Today, much of the country's power and energy is supplied by the private sector, whose business it is to provide services, and who has a vested interest in ensuring the continuity

of its business. The government must now work with the private sector to build data sharing alliances to protect citizens, property, and the economic sustainability of the United States.

Emergency Operations Centers

The Emergency Operations Center (EOC) is an essential component in a community's response program when an event escalates beyond the agency's capabilities. The operations within an EOC are increasingly dependent on GIS. The EOC plays a critical role in helping incident command manage the response and maintain continuity of operations for the remainder of the community. The EOC becomes the hub of government during a crisis. Department heads and other key decision makers come together to learn the effects of the incident, take actions to contain the emergency, and maintain government operations. Information and current situational awareness are essential for decision makers to be effective. GIS is rapidly becoming the platform that integrates dynamic information and displays the location of events and their impacts. Real-time knowledge, such as the location of resource deployments, areas of worsening conditions, and locations of those who may be in harm's way, can be accurately disseminated as operational data generated by GIS and shared with multiple agencies or organizations for a coordinated response. As an incident escalates to the point it requires regional or national support, the operational data can provide a continuous common view of circumstances across multiple agencies.

Data Fusion Centers

The Department of Homeland Security is emphasizing the need for a systematic repository of intelligence data. The intelligence data is to be analyzed and shared with appropriate law enforcement agencies for tactical response if necessary.

One of the many challenges associated with combining disparate data sources, better known as data fusion, is creating the relationship between the data schemas. There are numerous data schema methods, so trying to make sense of the relationships between them is a daunting task.

For example, when determining the relationship between bus routes and recent criminal activity, it may appear on the surface that there is no relationship between the two datasets. However, if both datasets were spatially referenced, the data can be related based on its location. With that said, if a series of convenience store robberies occurs along a given bus route during a specific time of day, a correlation can be made to someone who typically rides that route. This information could be given to law enforcement agencies to increase patrols appropriately to prevent future robberies.

Therefore, organizing data using a Location, Alphabetical, Time, Category, Hierarchy (LATCH) data schema, with location being the most common reference, is more valuable in fusing and presenting the data.

State and local records management systems are an excellent place to begin when determining a data fusion strategy or methodology. Often, a state or local RMS repository of crime and incident data contains a master indexing schema, which is usually spatially referenced. Today, many RMS solutions contain automatic geocoding capabilities that geospatially enable incident data stored in the data warehouse. This trend is being driven by market demand as the power of GIS and data fusion are understood. Data fusion centers are challenged with acquiring data in a variety of formats from a variety of sources and quickly integrating this data into meaningful, actionable information to

prevent crimes and attacks and apprehend perpetrators. GIS provides data fusion centers with powerful tools to meet these challenges.

Response Exercises

Response exercises, commonly known as response drills, are an essential part of preparedness and are valuable in identifying strengths and weaknesses in any response plan. Exercises are often followed by a debriefing session whereby observers and participants critique the event and discuss what went well, what did not, and what improvements are needed. Effective exercises often involve multiple agencies and departments.

Today, technology can facilitate exercises that represent many elements of a traditional drill virtually.

Virtual exercising is the utilization of software to conduct an analysis of potential outcomes prior to investing time and materials to perform a physical drill. Virtual exercising essentially supplements the physical exercise by providing better up-front planning of the drill itself. Virtual exercises can test variables that are otherwise too difficult, costly, or unsafe to simulate in a live scenario.

GIS enhances virtual and physical response exercises by geographically pinpointing and visually displaying threats and hazards in conjunction with other geographic data, such as population density, critical infrastructure locations, resource placement/deployment locations, and transportation routes, to better understand risks to life, health, and property as well as economic impacts.

One of the primary staples of command and control at the tactical incident level is the development of an incident action plan. This plan is communicated to key emergency management personnel, who supervise the implementation of the plan to control the incident. The communication of the incident action plan is customarily done through a briefing with maps of the incident. These maps create a common view of the problem and a common understanding of what actions are required to address priority problems. GIS is effective at creating the briefing map as well as other important incident maps including

- Incident transportation maps
- Incident perimeter and incident command system (ICS) branches, divisions, and facilities
- Logistical supply points, drop points, and fueling areas
- Incident air traffic patterns
- Incident models and predictions
- Hazard areas and hot zones

During exercises, GIS can play a vital role in helping incident management personnel better understand how events may unfold, potential consequences, and effective actions necessary to control an incident.

J-9652

Conclusion

For many years, GIS was seen as a tool that was strictly used by people who take care of streets or community planning. In the realm of public safety, GIS was merely thought of as "my map" or "a means of finding my way." Today, however, GIS is increasingly becoming part of an overall IT strategy for information authoring, publishing, and consuming.

The value of GIS in a homeland security data fusion strategy is demonstrated through the ability to organize and analyze authoritative data based on a location reference. ArcGIS Server supports a service-oriented architecture, which enables critical and sensitive information to be accessible to and shared with anyone who has security authentication, improving the likelihood of an effective response to a security threat or catastrophic event.

Protecting the nation's critical infrastructure is as much an outcome of good analysis and planning as it is an exercise in collecting information. ArcPad® provides functionality for DHS field personnel to accurately pinpoint the location of critical assets using a wireless handheld device. They are then able to upload the data to ArcGIS Server, where the data can be analyzed for potential threats or used in response planning. The first necessity in critical infrastructure protection is knowing where the assets and resources are located.

There are five key components to any internal technology solution: hardware, software, networks, data repositories, and trained users. GIS tools today are increasingly adding value in the desktop and mobile environments by presenting information in the context of its location. Everything that occurs does so at a specific point on earth. Geoanalysis using GIS technology provides the ability to understand potential relationships between data. Spatially enabled devices, networks, and applications provide a higher degree of intelligence and capability to the system because of the fundamental understanding of how location affects business and process decisions.

Whether the homeland security need is in Emergency Operations Centers solving complex problems, in intelligence centers analyzing threats and risks, in administration offices creating strategic plans, or in the field coordinating multiagency response and recovery efforts, GIS is sure to add value by giving geographic insight to those who need to make tough decisions for a secure homeland.