1
Gathering and analyzing intelligence

Homeland security intelligence is more about bits and bytes than cloaks and daggers these days, and GIS is the core technology for collecting, analyzing, and visualizing spatial data. Tom Ridge, the first U.S. secretary of Homeland Security, pictured an ideal counterterrorism computer network linking federal, state, and local intelligence and law enforcement agencies so they could instantaneously share threat reports, investigative leads, and potential evidence.

"In this new post-9-11 era, a new philosophy is required—a philosophy of shared responsibility, shared leadership and shared accountability," Ridge said in 2004 when he announced the creation of a national intelligence network. "The federal government cannot micromanage the protection of America."[1]

1. Spencer S. Hsu, "Anti-Terrorism Network Launched. System Allows Agencies Across Country to Share Data Instantaneously." *The Washington Post*, February 25, 2004, B01.

Computer technology, principally GIS, helps government officials monitor crimes and suspicious activity suggesting terrorism. Collecting and fusing spatial data from a broad array of sources is the backbone of contemporary antiterrorism intelligence. Data sources consist of official law enforcement intelligence along with general information from other government agencies and the private sector. Data fusion supports risk-based, information-driven programs of prevention and response to emerging or immediate threats, be they plots by humans or forces of nature.

Surveillance and response

In the areas of surveillance and detection, GIS can help law enforcement and intelligence officials grasp risky situations by assessing time-and-space relationships, recognizing patterns, and correlating seemingly disconnected events. Digital mapping coordinates surveillance and detection while the analytical capabilities of GIS help decision makers take defensive or preemptive action. A geographic analysis can track the movements of suspicious people, mobilize resources efficiently to prevent a terrorist event or minimize consequences, and determine an area's vulnerability to bioterrorism.

Increasingly sophisticated information-gathering systems, from covert sensors to satellite communications interceptors, generate huge volumes of data much like pieces of a jigsaw puzzle. The integrating power of GIS can create a vivid panorama. When threat data is matched with geographic data, GIS can document the convergence of location, vulnerability, high risk, suspects, and events. Statewide organizations such as the California Anti-Terrorism Information Center, established shortly after the September 11 attacks, and the Arizona Counter Terrorism Information Center, formed in 2004, have emerged as models for multifaceted intelligence processing powered by GIS.

Secure data sharing

The premise of the Department of Homeland Security's intelligence-sharing policy is that a widespread Internet-based network must be easily accessible through official channels yet secure enough to prevent sensitive information from getting into the wrong hands. Sharing geographic data in an open society raised concerns that potential terrorists could exploit this information. But a 2004 study by RAND, the California think tank, concluded that there was no need to impose broad restrictions on digital geographic data. The study found that the vast majority of federal datasets are of little use to an attacker or are available from so many other nongovernment sources that limiting access would be pointless. The study further found that data sharing is good for the economy as well as homeland security.

Intelligence gathering and analysis pays dividends to state and local governments beyond terrorism awareness. The process strengthens their ability to identify and forecast emerging crime, public health, and quality-of-life trends; supports targeted law enforcement and other problem-solving activities customized to local communities; and improves emergency and nonemergency services.

As outlined by the U.S. Homeland Security Advisory Council in 2005, effective intelligence fusion requires common terminology, definitions, and lexicon; a shared understanding of the threat environment and indicators of an emerging threat; coordination with federal intelligence and law enforcement entities on information-gathering protocols; and clear delineation of roles, responsibilities, and requirements at each level involved in the fusion process.

The president and Congress called for establishing an "information sharing environment" in which data fusion and collaboration activities within the federal government and among federal, state, local, tribal, and private entities carry out the homeland security mission.

Such an environment not only involves law enforcement, and state and regional intelligence centers, but also a general public educated on what suspicious activity or circumstances to look for and what to do with that information.

CASE STUDY

Emergency Management Mapping Application (EMMA)

A densely populated region containing the seat of federal government, financial centers, and numerous high-tech companies requires exceptional safeguarding from terrorist acts and natural disasters. Maryland and the National Capital Region have put their trust in the Emergency Management Mapping Application (EMMA). The data fusion software provides the tools to pinpoint an incident, generate a location report with a visual display, analyze an affected area, and coordinate resources. EMMA fosters communication among disparate agencies and assists emergency crews in the field by creating a common operating picture.

EMMA, shorthand for the Emergency Management Mapping Application data fusion software, is a vital tool for homeland security officials responsible for protecting the National Capital Region.

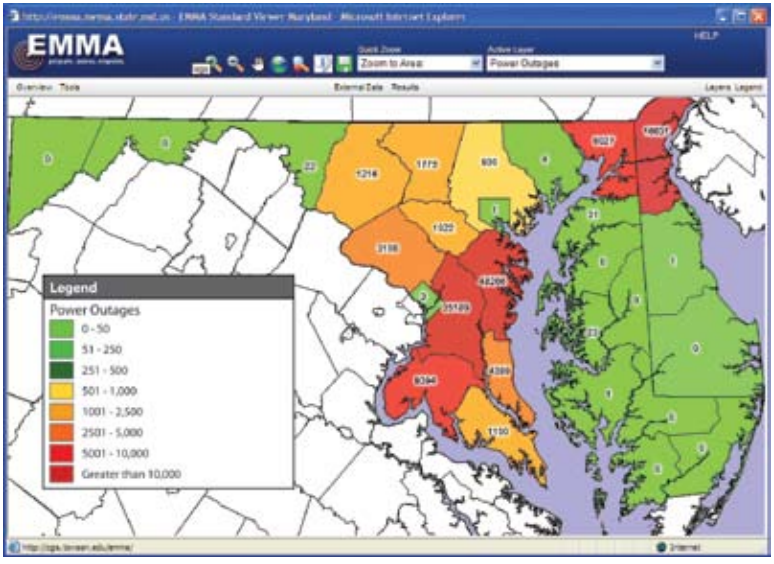
Comstock/Comstock Images: Government & Social Issues/ Jupiterimages.

The Web-based GIS enterprise system was developed at Towson University. It is built on a Java framework and integrates various ESRI-based mapping capabilities that follow industry standards. EMMA is installed at the Maryland State Emergency Operations Center and allows users to access various databases through interactive maps. EMMA's interoperability benefits dozens of cities, counties, police departments, and transportation agencies in the region. That technological edge has resulted in coordinated action across all levels of government.

Towson creates EMMA

The Center for Geographic Information Sciences (CGIS) at Towson University near Baltimore, Maryland, created EMMA in 2003 for the Maryland Emergency Management Agency to satisfy the need for mapping technologies that save time and lives. That year, Hurricane Isabel unleashed fierce winds and storm surge flooding. Within minutes, EMMA determined where to place sandbags at the Frederick County reservoir, a task that would have taken hours in the field.

In 2005, the U.S. Department of Homeland Security's Information Technology Evaluation Program funded a pilot effort called the Maryland Emergency Geographic Information Network (MEGIN). Led by Towson University, the pilot established technology for securely sharing data across organizational, jurisdictional, and disciplinary boundaries. MEGIN is Maryland's vision for a secure, coordinated information portal for the emergency management community, whose goal is to get the right data to the right person at the right time. MEGIN comprises ESRI's Portal Toolkit with an added measure of security at multiple levels, as well as a process for data owners to securely share map services with regional partners.



EMMA integrates real-time power outage information across Maryland. This map was produced during a 2007 ice storm.

Sources: Matthew Felton, Towson University; Maryland Emergency Management Agency.

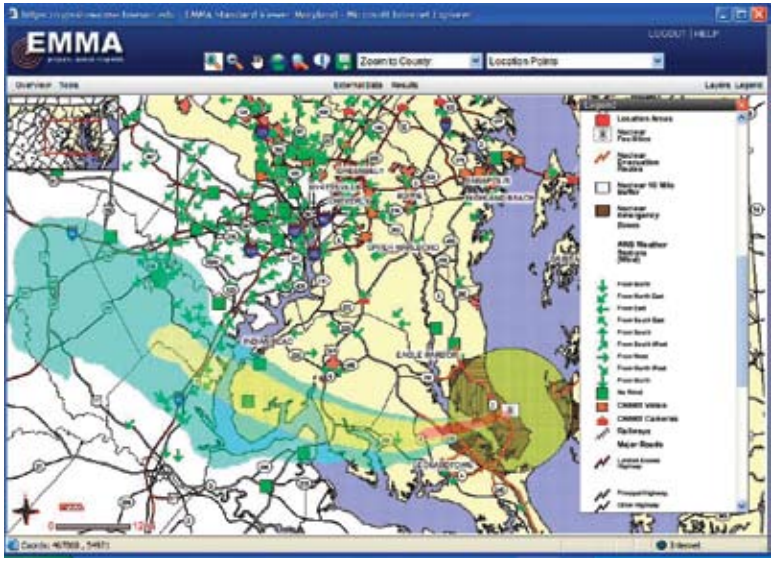
EMMA is fully interoperable with other GIS software and with incident management software. Its modular system architecture allows for flexibility and expandability, so as more maps are needed, more servers can be used for both database and application scalability. EMMA incorporates the Open GIS Consortium (OGC) Web Map Services (WMS) standard, which is an XML- and URL-based schema for providing and retrieving map services across multiple platforms.

In an emergency situation, EMMA pulls data from various agencies and weaves it into a single interactive map. First responders have access to crucial resources, such as nearest police and fire departments, vulnerable areas, and local geography. EMMA's real-time capabilities include determining a particular hospital's available beds, calling up current weather conditions, and pinpointing the location of individual patrol cars. When hazardous materials spill on the highway, EMMA tells users the direction and speed of the wind, which schools are in harm's way, and what roads need to be closed.

The reach of EMMA

EMMA is tied to several federal and state GIS initiatives, including the U.S. Geological Survey's National Map project and Geospatial One-Stop, the Web-based data exchange program. EMMA plays an important role in developing mitigation plans for critical infrastructure, modeling emergency events, and response plans. CGIS has worked closely with the State Emergency Operations Center (SEOC) to put technologies and processes in place that significantly increase Maryland's preparedness for large-scale natural or terrorist disasters.

In 2005, Maryland relief officials were deployed to the Gulf Coast region devastated by Hurricane Katrina. Response teams found themselves in unfamiliar territory and with limited communications. EMMA proved to be the equalizer, coordinating the operation with



EMMA incorporates real-time weather and transportation data with a nuclear plume simulation in the National Capital region.

Sources: Matthew Felton, Towson University; AWS Convergence Technologies; Maryland Department of Transportation; National Oceanic and Atmospheric Administration.

dynamic maps. Dubbed "EMMA Katrina," the operation coordinated data for a broad area of the Gulf Region, and its integration with WebEOC allowed for the location of response teams to be tracked practically in real time.

Building on the success of Maryland's statewide implementation of EMMA, local implementations were rolled out to individual county jurisdictions in Maryland. In addition, several other states as well as local jurisdictions within the National Capital Region looked toward EMMA as a GIS solution to their emergency operations needs.

During the summer of 2006, a prototype implementation of EMMA dubbed "NCR Map" was deployed to demonstrate a regional implementation of EMMA in support of the GIS committee of the Metropolitan Washington Council of Governments (MWCOG). Shortly after this prototype was deployed, emergency management officials from Washington, D.C., used EMMA to understand the risk posed by a leaking dam several miles north of their jurisdiction in Rockville, Maryland. Rather than requesting this data and importing into their GIS, Washington, D.C., officials simply launched EMMA and focused on the area at risk.

Reusability

EMMA's latest release, version 2.0, focuses on increased security and interoperability, additional tools, and an expanded database. Future versions of EMMA will be designed to access information such as geospatial metadata through MEGIN by providing a search engine.

In February 2006, both EMMA and MEGIN were evaluated by independent consultants from the National Capital Region who assessed the technical reusability of various programs in the region. As part of this process, EMMA and MEGIN technology was measured against the federal government's Technical Reference Model (TRM), a part of the E-GOV initiative that provides a foundation to categorize the standards, specifications, and technologies to support the construction, delivery, and exchange of business and application components. EMMA and MEGIN technology received very high marks in this evaluation, which verified its reusability for a broad range of applications.

CASE STUDY

South Carolina Information Exchange (SCIEx)

Geospatial technology has the capacity to transform accumulated information into valuable intelligence for enforcing the law and protecting the homeland. That's exactly what has happened in South Carolina where a grassroots cooperative among sheriffs and police chiefs in 2001 blossomed into a statewide model for intelligence fusion.

After the September 11 attacks, South Carolina's state and local law enforcement community saw the need for a system to gather information from diverse, statewide resources and make the data available to the intelligence process. To develop actionable intelligence, analysts must have data in useable formats from as wide a universe of

resources as practical and pertinent. This capability was largely missing or fractured around South Carolina's agencies and local jurisdictions.

A proactive approach

The South Carolina Law Enforcement Division (SLED) set out to develop an information technology system to support the intelligence process. Its mission would be to take a proactive approach to collecting, displaying, analyzing, and acting on intelligence in order to detect and prevent terrorist acts and precursor crimes such as money laundering, identity theft, narcotics, and smuggling.

In March 2005, the South Carolina Information Exchange (SCIEx) was conceptualized and initiated. It would consist of the SCIEx Intelligence Fusion Center and the SCIEx Data Warehouse project. An open-source model for sharing law enforcement records management system (RMS) incident information in Charleston—in which six agencies in a four-county area shared incident data electronically across jurisdictional boundaries—was adopted as the core technology to develop and expand statewide.

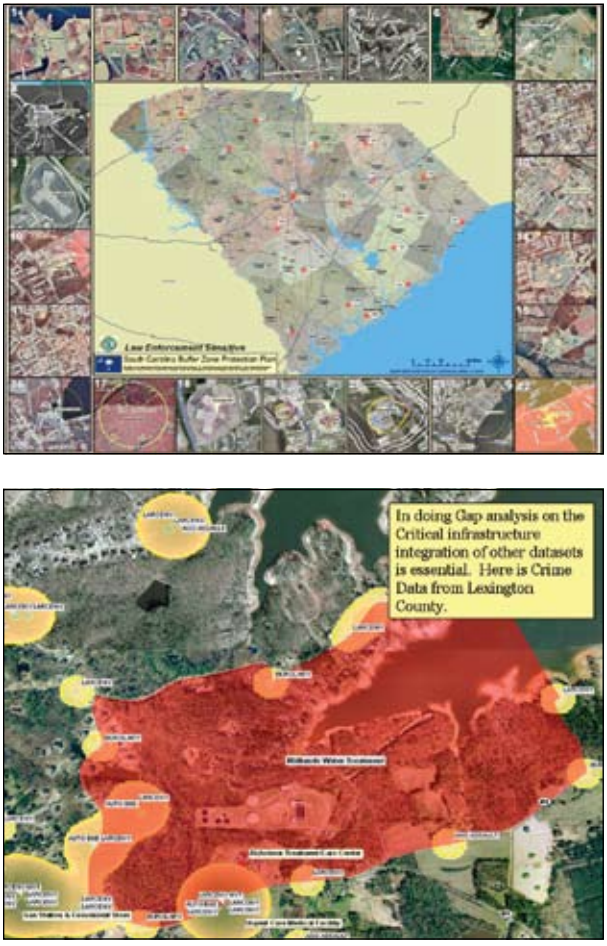
The task was significant, in that South Carolina has over 275 law enforcement jurisdictions and over twenty RMS application vendors with active accounts in the state. SLED contracted with the developers of the model, the National Law Enforcement Corrections and Technology Center-Southeast (NLECTC-SE) and Scientific Research Corporation (SRC) to continue to expand and grow the systems capabilities and footprint. The system currently has more than 150 agencies replicating incident data to the warehouse and using the system in the conduct of investigations.

GIS joins the picture

Early in the development of the SCIEx project it was determined that GIS would be invaluable for the display and analysis of the raw incident data. SLED turned to ESRI and its business partner the Omega Group, a San Diego–based GIS specialist for law enforcement, and they teamed with SRC to implement the geospatial component of SCIEx. The technical team first geocoded all crime data stored in the SCIEx warehouse and designed a process for geocoding new crimes entered into the system. The Omega Group's CrimeView analytical software then examined the geocoded data for trend analysis, querying, and reporting.

A common operational picture (COP) situation map was developed to display incidents and data layers on the fusion center video wall. Near-real-time incidents were displayed against layers of critical infrastructure, potential targets, areas of interest or activity, and other datasets collected from around the state. Because the system was open and scaleable, SCIEx was able to integrate the state's sex offender dataset into the central data warehouse and worked toward adding many more datasets.

South Carolina is one of thirteen states committed to a homeland security initiative called Southern Shield. Relying on GIS, the member states exchange best practices, share terrorism-related intelligence, and monitor regional terrorism threats. The Global Justice XML data reference model, sponsored by the U.S. Department of Justice, has facilitated the interstate and federal collaboration.



South Carolina law enforcement relies on GIS to coordinate intelligence and data on crime and infrastructure to provide a clear picture of threats and potential targets.

Source: South Carolina Law Enforcement Division.

SCIEx would be expanded to include data from corrections and jail entities, computer-aided dispatch systems, the court system, and a host of other state agency data. The SCIEx Fusion Center also planned to introduce Pictometry technology—oblique aerial photography integrated with GIS—for critical infrastructure protection and response, and in support of operations like natural disaster recovery and major event security.

Captain Teresa Woods of the South Carolina Law Enforcement Division was principal contributor to this case study.

CASE STUDY

Arizona Counter Terrorism Information Center (ACTIC)

Arizona's counterterrorism network combines high-tech processes with grassroots participation to secure a vulnerable corner of America's homeland. The Arizona Counter Terrorism Information Center (ACTIC) is the state's analysis hub for crime- and terrorism-related intelligence and is staffed by two hundred representatives of local, state, and federal law enforcement agencies. Based in Phoenix, ACTIC has investigated security breaches at Sky Harbor International Airport, an attempt to manufacture the biological toxin ricin, and suspicious international border crossings. A $5.3 million Department of Homeland Security grant in 2004 established the center, hailed as a model for cooperative interagency law enforcement.

A dynamic data fusion system is ACTIC's most potent weapon in its mission to detect, prevent, and respond to terrorism and other critical events. The system, powered by ArcGIS software and MetaCarta's Geographic Text Search (GTS), combines structured intelligence and spatial data with such unstructured content as e-mail, Web pages, and news articles, enriching intelligence for field agents.

Tapping unstructured information sources

GTS automatically extracts geographic references from unstructured text and plots documents on a map. Analysts can search text archives using keywords and geographic extents as filters. Without this capability, analysts would spend hours pouring over documents relevant to the area in question. ACTIC agents routinely use GTS technology to check public sources of unstructured information, such as American and Mexican newspaper Web pages, when gathering intelligence about a specific location. So, when law enforcement responds to an incident, officers instantly know what has happened in the

The Arizona Counter Terrorism Information Center gathers intelligence to protect the state, including its vast reaches of hostile desert.

Photo 24/BrandX: National Parks/ Jupiterimages.

Surveillance along the Arizona border includes use of unmanned aerial vehicles equipped with electro-optic sensors and communications equipment to provide around-the-clock images to Border Patrol agents.

Source: U.S. Department of Homeland Security.

neighborhood that has made news or drawn the attention of other agencies. MetaCarta officials and law enforcement authorities estimate that 80 percent of intelligence relevant to law enforcement is unstructured content.

Similar to the Neighborhood Watch concept, ACTIC encourages citizens to be vigilant and report any suspicious activity. As terrorists focus on buses, trains, public gathering spots, and other "soft targets," ACTIC relies on ordinary citizens to step up as the eyes and ears of the community.

Sharing the data

Calls to the center are assigned to an agent who logs the report into a database and refers it to the appropriate department, be it the bomb squad or counterterrorism unit, to determine if the threat is legitimate. From that point on, all public safety agencies from the federal government to the local fire departments have access to the same data. Before ACTIC, the data information systems of various law enforcement entities were not linked, making it difficult to track suspicious trends or recognize a pending terrorist threat.

Government intelligence reports consider Arizona's 370-mile international border to be vulnerable to terrorist penetration, so that stretch of desert is patrolled by some 2,400 agents and civilian volunteers. Law enforcement officials say that while al-Qaeda appears to favor safer, easier routes into the United States over Arizona's harsh southern boundary, the threat remains real. Border control has been beefed up dramatically since September 11, with more labor and technology focusing on antiterrorism. Agents are trained to spot non-Mexicans and turn suspicious border crossers over to the FBI for questioning.

ACTIC also assists the private sector's contribution to homeland security. The center created an information-sharing and training program for about 19,000 security officers

attached to 201 private companies throughout Arizona. Homeland defense experts say that private security companies protect three-fourths of the nation's most likely targets for terrorism. Arizona relies on private security to patrol dam sites and airport perimeters, protect the state's nuclear power plant, and guard banks. In 2002, state officials toughened standards for private security guards and boosted their role as community sentinels who have access to shared law enforcement intelligence and are plugged into the alert system when threats arise.

References

Arizona Counter Terrorism Information Center Web site. http://www.nga.org/cda/files/0405BioterrorismPhelps.ppt.

Baker, John C., et. al. 2004. *Mapping the risks: Assessing the homeland security implications of publicly available geospatial information.* Santa Monica, Calif.: RAND Corporation.

Coleman, Kevin. 2003. GIS, information technology, and biotech take center stage in supporting homeland security. *Directions Magazine,* April 11. http://www.locationintelligence.net/articles/345.html.

E-Gov. Federal Enterprise Architecture. http://www.whitehouse.gov/omb/egov/a-6-trm.html.

Felton, Matthew, and John Morgan. 2004. Emergency management mapping application: Integrating data online for emergency management. Paper presented at the twenty-fifth annual ESRI International User Conference, August 9–13, San Diego, California.

GIS for Emergency Management in Maryland. 2004. EMMA: Emergency Management Mapping Application Towson University Center for Geographic Information Services Quarterly Newsletter, spring. http://cgis.towson.edu/newsletter/newsletter_spring_04_emma.htm.

Hensley, J. J. 2005. Phoenix center a hub for coordinating terrorism data. *The Arizona Republic,* July 9. http://www.azcentral.com/arizonarepublic/local/articles/0709counterterror.html.

Justice Technology Information Network Web site. South Carolina Information Exchange PowerPoint presentation. www.justnet.org/nlectcse/download/knight_sciex_sccjis2006.ppt.

Knight, Coleman. Statewide information sharing in South Carolina. 2006. *The Police Chief* vol. 73, no. 4 (April). http://policechiefmagazine.org/magazine/index cfm?fuseaction=display_arch&article_id=856&issue_id=42006.

Maryland Governor's Office of Homeland Security. 2005. *Public Safety Communications Interoperability in Maryland.* MD-IPT-RPT-R3CI. February 28.

Ridley, Randy, and John-Henry Gross. 2005. Preventing terrorism with geographic text searches. *ArcUser Online* April–June. http://gis.esri.com/library/userconf/proc04/docs/pap1430.pdf.

Ridley, Randy, and Mike Odell. 2005. Interview by Matteo Luccio, *GIS Monitor newsletter.* August 11. http://www.gismonitor.com/news/newsletter/archive/081105.php.

Romeo, Jim. 2005. Arizona gets a better view. *Emergency, Fire/Rescue & Police Magazine.* http://www.efpmagazine.com/Technology/MetaCarta.asp (accessed July 12, 2006).

SCRA Web site. Information is the key to security. http://www.scra.org/homeland_security.shtml.

South Carolina Law Enforcement Division. 2006. *2005–2006 Annual Accountability Report.*

Thorlin, Scott. Setting the table for information sharing: Would you please pass the intelligence? December 27, 2004, interview on FBI Web site. http://www.fbi.gov/page2/dec04/actic122704.htm.

Towson University Center for Geographic Information Services Web site. 2004. Fire? Flood? Rescue workers use TU's new CGIS mapping tool. *Tech Talk* March 29. wwwnew.towson.edu/techtalk/20040329,1_techTalkArticle.html.

———. EMMA: Prepare, assess, respond. http://cgis.towson.edu/downloads/EMMA_whitepaper.pdf.

U.S. Department of Homeland Security. Homeland Security Advisory Council. 2005. *Intelligence and Information Sharing Initiative: Homeland Security Intelligence & Information Fusion.* April 28.

Wagner, Dennis. 2004. Border no terror corridor—so far: Still, infiltration threat via Mexico called real. *The Arizona Republic,* August 22. http://www.azcentral.com/arizonarepublic/news/articles/0822borderterror23.html.

———. 2006. Private security guards play key roles post-9/11. *The Arizona Republic,* January 22. http://www.azcentral.com/arizonarepublic/news/articles/0122privatesecurity.html.