

INFRASTRUCTURE VULNERABILITY PROTECTION GIS TOOLS

BIOGRAPHICAL INFORMATION

Roxanne Cox-Drake
Electric & Gas Industry Manager
ESRI

Specific Responsibilities

Roxanne Cox-Drake is currently an Industry Solutions Manager at ESRI, supporting the Electric & Gas Utility market and responsible for customers feedback and satisfaction, developing business partnerships, influencing product development and supporting the regional and international sales people with marketing strategies and materials for electric & gas utilities.

Past Experience

Previously, as Senior Technology Manager at Southern California Edison (SCE), Roxanne's responsibilities included integration of business processes and systems for Distribution and Transmission, technology to support Distribution Automation, maintenance management and related systems for nuclear generation and other corporate systems and services, such as human resources and benefits systems, Technology Operations Center and helpdesk, desktop support services and the corporate assessment for comprehensive outsourcing of IT services.

Other developed expertise includes organizational assessment and design and large team facilitation for business process improvement and work group integration. While these transferable skills were developed working on process improvement and cross-departmental initiatives at SCE they are regularly utilized by ESRI and the ESRI Electric & Gas User Group community.

Educational Information

Roxanne graduated with a Bachelor of Science in Business Administration, with a major in Information Systems from California Polytechnic University, Pomona, California. She also completed the Executive Management Program at University of California, Riverside.

Professional Memberships

Roxanne is a member of the Geospatial Information technology Association (GITA) and serves as Co-Chair for the Education Committee.

INFRASTRUCTURE VULNERABILITY PROTECTION GIS TOOLS

Roxanne Cox-Drake
ESRI
380 New York St.
Redlands, CA 92373

ABSTRACT

GIS is a key component of the US Government's approach to homeland security. After defining homeland security with respect to critical infrastructure and presenting a framework for analyzing infrastructure vulnerability, this paper will discuss what this means for utilities and how they may take advantage of various programs and initiatives to protect their own assets.

BACKGROUND

Thousands of sites and facilities and hundreds of thousands of miles of pipelines and distribution networks crisscross this country supplying the nation with necessities of life, and commerce. Ownership and custodianship of this infrastructure is in the hands of private industry, public utilities, municipalities, and various levels of government. Much of this infrastructure is defined and documented in GIS systems. This information has been assembled and maintained to support asset management, maintenance, lease, and operational functions of the organization, all-important business functions supported with commercial and custom GIS solutions.

These infrastructures face risks from both natural and manmade threats that can result in infrastructure damage or loss; catastrophic impacts on surrounding areas and populations; failure of delivery of services or supplies; and potentially severe impacts on other critical infrastructure, sites, and/or operations.

Protecting infrastructure involves many overlapping functions. Vulnerability assessment is one of the foundation functions. Other necessary functions required to protect infrastructure include threat detection, target hardening, threat deterrence, consequence planning, response, and recovery. Those functions won't be covered in this discussion. However, they ultimately rely on sound vulnerability assessment.

TOOLS SUPPORTING INFRASTRUCTURE VULNERABILITY ASSESSMENT

This discussion focuses on geospatial tools to assist an organization to perform vulnerability assessments of its infrastructure.

GIS is a solid foundation to undertake infrastructure vulnerability assessments and the concepts and prototypes of these tools will be covered in this discussion. A tool set which assists during the vulnerability assessment process will form the foundation for security decisions, hardening investments and reduce the intra and inter inconsistencies between

sectors and stakeholders. The results of assessments undertaken with the tool set will be able to contribute to a complete common operating picture (COP) and situational awareness for infrastructure owners, regulators, and appropriate levels of government.

Characteristics of a tool set would include integration with an existing enterprise GIS or the ability to run in a stand-alone mode. Web services, facilitate data collection and multi jurisdictional data sharing would also be important as applicable.

A tool set would not accomplish all the functions required to secure infrastructure, but activities related to the initial vulnerability assessment stage. What is needed are tools and processes to:

- Establish an Infrastructure Data Model
- Establish Infrastructure Templates
- Establish Hazards Templates for both natural and manmade hazards
- Support vulnerability analyses
- Present vulnerabilities in a logical and easily recognizable context
- Support export and interface to other tools and systems that provide other functionality such as:
 - Automated Incident Input for Threat/Hazard Monitoring & Correlation
 - Alert, Warning, and Communication System(s)
 - Natural and Manmade Hazard Modeling

Data Model

To undertake infrastructure vulnerability assessments requires knowledge of the geospatial environment in which prevention of natural, technological, and terrorist events would take place. This involves developing a clear picture of the geographic features, underlying infrastructure and geologic structure, the built environment, and demographics of the region or site. Geographic Information Systems (GIS) can provide this understanding in maps, multi-spectral satellite images, and geo-referenced video, voice and digital photos.

Institutions have been collecting this information for years for various purposes. In some cases this data is stored in separate systems and in others its part of an enterprise GIS. Interested participants and government sponsorship is undertaking a homeland security data model development effort. This model is intended to be adaptable to an organization's needs and most importantly specify data required to perform vulnerability assessments. This is intended to be an evolutionary process with refinements being made to the model.

Participation is open and information can be obtained at:

<http://downloads.esri.com/support/datamodels/Homeland%20Security/HLS.zip>

The model should include data stores for assets, relationships of assets to specific operations, business logic, vulnerability information and other relevant data needed to run analyses within the tool set.

Infrastructure Templates

Templates are needed to assist in the identification and sourcing of data required for

vulnerability assessments. As with the data model effort, these templates should be dynamic, refined and modified by industries and jurisdictions based on their needs and experiences.

Hazard(s) Templates (Natural and Manmade)

Other templates are needed to support the documentation and identification of threats and hazards. Natural threat templates may include wildfire, flood, earthquake, or other phenomena and would be completed based on infrastructure location and historical data. Manmade threat templates should be developed based on current threat data.

Vulnerability Analysis

The tool set supports infrastructure decomposition and identification of key sites, components, and resources. It identifies infrastructure or resources that are critical to ensure peak and sufficient operations. For example in a water system vulnerability assessment, the tool must have the flexibility to identify inputs that are critical to supporting key functions (eg. power to run a pump house, chlorine supply to treat the water). A comprehensive assessment must include an analysis and assessment of the supporting infrastructures. A clear vulnerability picture cannot be built without considering critical dependencies on supporting infrastructures. GIS-based analysis methods help to identify candidate assets, including:

- Network Analysis – Various network algorithms are applicable to trace critical infrastructure networks and identify assets that perform critical operations with individual networks. Such algorithms include shortest path, K-disjoint, max flow/min cut, minimal spanning tree and Steiner tree. These algorithms provide the basic computational foundation to analyze infrastructure networks but it is necessary to understand and apply standard infrastructure business rules to properly program networks for analysis. The business rules vary greatly across infrastructure. For example, electric power networks can be analyzed using the standard principles of an electrical generation station or network engineering while accounting for factors such as seasonal demand. We envision functionality encapsulating standard network algorithms coupled with relevant business rules to create industry unique analysis capabilities.
- Service Area Identification – For those infrastructures for which it is appropriate, it is then necessary to identify service area for critical assets. This step is necessary to identify subsequent interdependency analysis and also because changes elsewhere in a service area may affect the ability of an asset to effectively supply its infrastructure commodity. The methods for identifying services areas vary by infrastructure. For instance, telecommunications service areas are typically determined by service providers, based on market considerations. As a result, there are commercially available GIS data sets that depict service area polygons for many types of assets. For example, there are several data sets available that depict

infrastructures, such as electric power, service areas. For these infrastructures, geo-processing methods can be especially effective for calculating service area. Specifically, Voronoi diagrams (Theissen polygons) are particularly useful for estimating service areas. Several tools are available at no cost for download from the web.

- Interdependency Analysis – At this point we have characterized individual infrastructures as discrete entities, identifying those assets that are most likely critical operations. GIS provides a means to be able to investigate the incorporation of agent-based models to simulate the behaviors of infrastructure assets over time based on changes to their environment.

Presentation/Output

Analysis results are needed to for easy interpretation by analysts, decision makers, and security personnel. A GIS-based tool set provides several options for presenting and reporting results.

Future Considerations

Real Time Threat Update: The government has established several threat notification and collaboration systems including:

- the Homeland Security Information Network (HSIN)
- Joint Regional Information Exchange (JRIES)
- RISS-AIX
- Industry specific ISACs

Future upgrades to the tool set could incorporate direct connections to these systems and update the threat templates and assessments.

Interoperability with Other Tools: GIS helps manage threat data, facilitate reporting, visualize analysis results and many other key functions. A tool set should integrate with existing systems within an infrastructure organization to maximize the investments made in information stores across an enterprise.

SUMMARY

Infrastructure owners and the government do not have the resources or money to protect their entire infrastructure. Choices must be made about where to apply resources. A vulnerability tool set, which can assist in the identification of what infrastructure most needs protection, is of value. The fact that much of the necessary information to utilize the tool set can be leveraged from existing enterprise GIS's in many cases is another important driver.

The GIS-based vulnerability assessment tool set we envision can be integrated with an enterprise GIS or stand alone. In this day and age of asymmetrical threats to your industry and infrastructure, consideration should be given to incorporating some if not all of the critical infrastructure protection functions into your enterprise. A tool set is needed and should interface with other enterprise systems as well as emergency management and security systems.