Assuring Port Operations by Analyzing Supporting Infrastructures with Geographic Information Systems

William Dollins
Senior GIS Architect
Mission & Operations Analysis Branch
Defense Program Office for Mission Assurance

Table of Contents

Table of Contents 2
Introduction 3
Scope 3
Infrastructure Vulnerability Assessment 4
The Pre-Visit Phase 4
Foundation Data Gathering 5
Infrastructure Characterization 5
The On-Site Phase 8
The Post-Visit Phase 11
Future Directions 14
Conclusion 15

Introduction

The Defense Program Office for Mission Assurance (DPO-MA), a component of the Naval Surface Warfare Center Dahlgren Division in Dahlgren, VA has been a leader in the area of critical infrastructure protection since the mid-1990s. DPO-MA has focused it activities around the concept of "mission assurance." DPO-MA analysts focus their attention on collections of infrastructure assets identified as supporting a specific mission or function. As a Department of Defense (DoD) program, attention is typically paid to classic military missions such as force projection, communications and sustainment.

As part of its overall role in critical infrastructure protection, the DPO-MA employs teams of analysts to perform vulnerability assessments on key infrastructure assets in order to provide an assessment of potential risks to the execution of a mission. As a mission is analyzed and decomposed, key sites and facilities are identified. Those sites are then characterized to identify which of the functions they perform provide specific support to the overall mission being analyzed.

It is not surprising that ports play a large role in supporting DoD operations, as they have done for all great military powers throughout history. The volume of cargo movement required to support a large-scale military operation cannot be accomplished without the use of one or more ports. As a result, port operations, such as the ability to load and unload cargo and munitions, can be a large functional focus of mission assurance. Their operations are dependent upon the availability of transportation, energy, fuel, information and communication services that are provided by networks of infrastructure assets that extend beyond the boundaries of the ports themselves. Therefore, a complete port security profile must include an analysis and assessment of these supporting infrastructures.

Given the inherent geographic nature of physical infrastructures, geographic information systems (GIS) provide an excellent environment in which to model, analyze and depict infrastructure assets. DPO-MA analysts have made use of GIS tools in their analysis work for most of the last decade and the GIS environment has evolved from a few free-standing GIS desktops to a full implementation of the ESRI enterprise GIS approach. This growth has tracked with the growth of DPO-MA and interest in infrastructure protection.

Scope

DPO-MA analyzes several different kinds of physical and logical infrastructures. Each of these infrastructures is an in-depth area of expertise on its own. This paper will not include a detailed discussion of any particular infrastructure but will instead focus on how GIS tools support the various analyst teams in general.

The full range of analysis and assessment activity involved in mission assurance is quite broad. This paper focuses on only one aspect of the analysis and assessment lifecycle: the vulnerability assessment of supporting infrastructures. Depending upon the scale of the mission being analyzed, numerous sites may be assessed. This paper will focus only on the activities surrounding the on-site vulnerability assessment and how GIS tools are used to support those activities.

Infrastructure Vulnerability Assessment

DPO-MA conducts infrastructure vulnerability assessments as part of an overall mission assurance analysis and assessment lifecycle. When facilities such as ports or military installations are identified as supporting mission execution, the surrounding infrastructures are analyzed to determine how they affect key facility operations.

Consideration of the infrastructure networks that support key assets is essential to ensure a full vulnerability assessment. Taking a mission-oriented view forces the assessors to look at an asset's operational requirements and identify ways in which operations can be degraded without directly attacking the asset itself. By examining the supporting infrastructure requirements of key assets, the view of vulnerability and therefore security moves beyond the traditional "guns, guards, and dogs" view of securing assets.

A key piece of the overall vulnerability assessment lifecycle is the on-site assessment. It can be broken down into three main phases: the pre-visit phase, the on-site phase and the post-visit phase. GIS tools play key roles in each of these phases, supporting preparation, execution and product generation. The follow sections discuss how GIS-based tools assist in the vulnerability assessment process at DPO-MA.

The Pre-Visit Phase

By far, the most visible portion of the vulnerability assessment process is the on-site phase of the assessment. It is important to realize, however, that a significant amount of preparatory work is required before sending an assessment team to a port. GIS tools add great value to many pre-assessment activities. The ultimate goal of pre-assessment is to give the assessment team as complete a picture of the port of interest as possible and infrastructure analysts have identified a complete GIS picture as an invaluable tool to help them prepare for a site visit. There are various activities that make up the pre-assessment phase. The relationship of GIS to these activities is discussed in the following sections.

Foundation Data Gathering

The first step toward building a complete picture of a port and its supporting infrastructure is the gathering of sufficient foundation GIS data. The term "foundation data" refers to more than just traditional basemap data sets. Foundation data also includes GIS data that depicts the supporting energy, transportation, communication, water and wastewater networks. Because no analysis is performed during this activity, it is necessary to capture a data in an area-of-interest that may greatly exceed that of the port facility. This provides a sufficient foundation to support the characterization of supporting infrastructure networks in future activities.

Infrastructure Characterization

Once a sufficient GIS foundation has been laid, it is possible to use several GIS-based analysis methods to produce a list of candidate assets that support specified port operations. Such methods include:

- Network Analysis – Various network algorithms are applicable to trace supporting infrastructure networks and identify assets that support port 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 electrical engineering while accounting for factors such as seasonal demand. On the other hand, commercial rail networks must be analyzed using Byzantine economic rules that apply weighting factors for track ownership, trackage rights, crew restrictions and other factors. In a properly modeled rail network, a correct result can be anything but intuitive.

  To support the analysis of various networks, DPO-MA developers have built ArcGIS-based tools using NetEngine to encapsulate standard network algorithms and couple them with relevant business rules to create extensions that provide quick analysis capabilities using various commercial and government-developed GIS data sets. These tools have been integrated into the Mission Assurance Tool Suite (MATS). The MATS analysis tools provide the capability to analyze road, rail, communications and fuel logistics networks. Other infrastructures are analyzed using other commercially available tools. The MATS tools allow an analyst to identify failure sets within an infrastructure. Failure sets are defined as the collection of infrastructure assets that, if removed, would deny the availability of the infrastructure to the port and potentially disrupt port operations.

Using ArcGIS-based network analysis tools allows infrastructure analysts to narrow the infrastructure picture down from the broad foundation picture to a list of discreet assets that have been determined to support port operations. This list of assets will be used to narrow the focus of the on-site assessment team. By using GIS-based tools, the analysts can capitalize on rich commercially available data sets and continue to work in a single analysis environment.

- Service Area Identification – For those infrastructures for which it is appropriate, it is then necessary to identify service area for assets that support port operations. This step is necessary to support 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 end office coverage areas.

  For other infrastructures, such as electric power, service areas can fluctuate based upon peak load conditions, seasonal demand and other factors. 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. For this type of calculation, there are several freely available tools, some of which can be found on ESRI's ArcScripts download web site.

- Interdependency Analysis – At this point we have characterized individual infrastructures as discreet entities, identifying those assets that most likely support port operations. (It is important to note that the support functions of an asset are not confirmed until after the on-site assessment.) It is now necessary to model infrastructure interdependencies in order to determine if disruptions in one network cause perturbations in others.

Here again, ArcGIS-based tools are useful. For the past four years, DPO-MA developers have teamed with developers at the Argonne National Laboratory to develop a modeling and simulation engine to model infrastructure interdependencies. This package, called SymSuite, uses agent-based modeling to simulate the behaviors of infrastructure assets over time based on changes to their environment.

SymSuite uses GIS data sets as a starting point for a model. The data sets are read to gather the features with an area-of-interest. These features and their attributes are used to instantiate agents in their initial states. Agents are best described as self-directed objects (as in object-oriented programming) that take action and perform functions based on the stimuli of other agents and the modeling environment. The agents then work toward a goal based upon their programming.

The SymSuite model, once initiated, runs in memory. Agent state is maintained within the model without the need to make constant read/write operations back to the source data sets. Once the model is started, the data sets are no longer read.

SymSuite uses ArcMap 8.3 as its visualization environment. As the model runs and agent state is updated, the changes are reflected visually on the map. Because no changes to the databases are being made, it is necessary to divorce the map rendering from the data sets. As a result, custom objects were developed to render map features based on the state of in-memory agents.

SymSuite uses personal geodatabases as working areas to maintain the interdependency linkages between infrastructure assets. In this manner relationships such as that between a power plant and its fuel sources are stored in order to support agent instantiation. As SymSuite executes a model, a perturbation in the natural gas infrastructure may affect the flow of fuel to a power plant. When the natural gas fuel flow drops below a certain threshold, the power plant agent will programmatically switch to its secondary fuel source, which may be a set of on-site oil storage tanks.

The interdependency relationships can be quantified using a series of methods ranging from high confidence (an explicit relationship established in a data set) to low confidence (a nearest-neighbor spatial relationship). The model result can help give assessors an idea of the behaviors and relationships between infrastructure networks in the vicinity of a port. It can also help identify potential assets of interest that may have been missed in earlier steps.

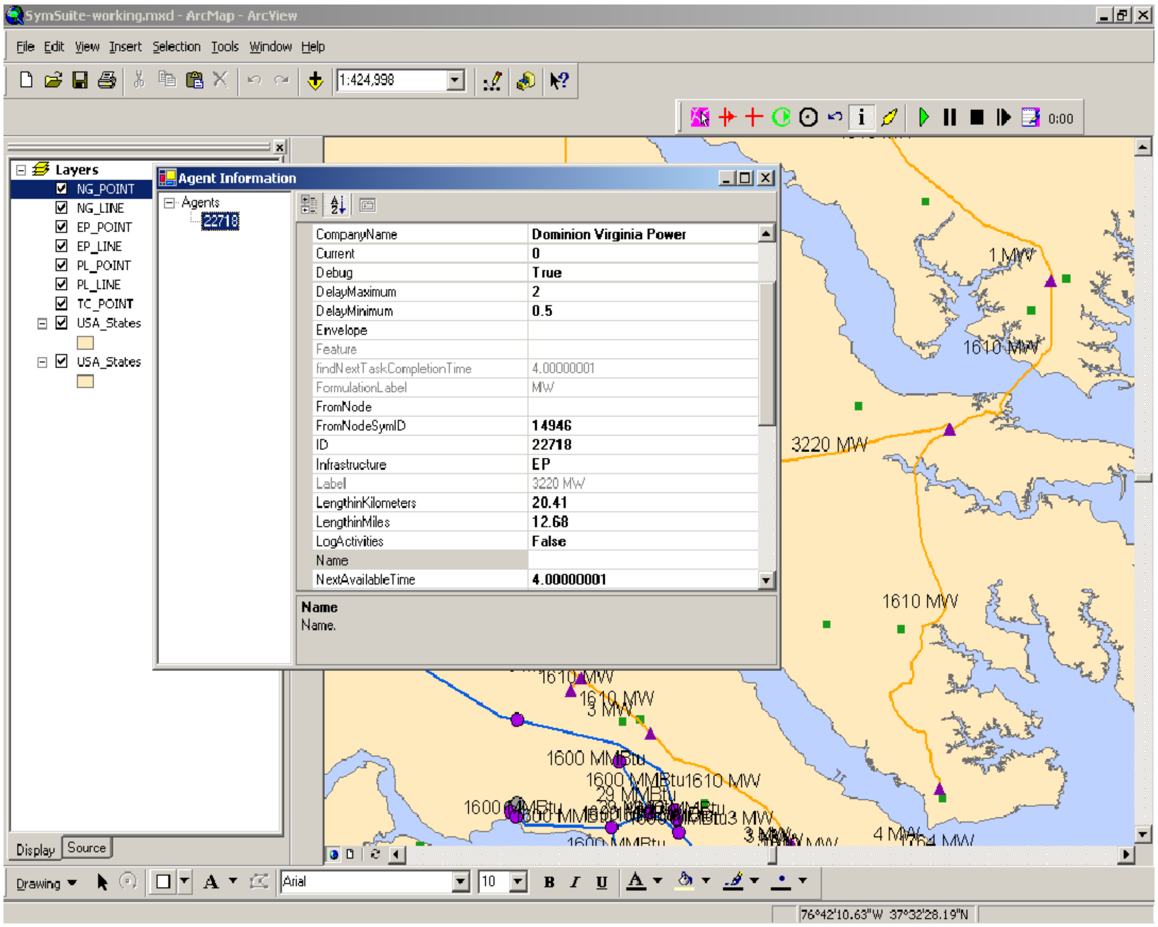

Figure 1: SymSuite AgentInfo tool queries agent state in a manner similar to the ArcMap identify tool.

The On-Site Phase

Once the various preparatory activities have been completed, it is time for the assessment team to visit the port of interest. There are numerous activities that are performed during course of a vulnerability assessment and there are several tools that are used. This section will deal only with those activities in which GIS tools play a significant role.

The purpose of the on-site vulnerability assessment is to accomplish the following tasks:

1. To verify the list of supporting assets identified in earlier stages. At this point, assets may be added or removed based upon “ground truth.”
2. To verify those supporting assets that comprise the failure sets for various infrastructures with respect to port operations.
3. To verify the interdependency relationships identified in earlier stages.
4. To verify certain properties of the assets, including location.
5. To gather information on the hazards, vulnerabilities and countermeasures that are applicable to the supporting infrastructure assets.

The DPO-MA has developed a relational database structure to collect and store the information collected during an assessment. This database, called the Defense Critical Infrastructure Program (DCIP) database stores the relationships of assets to the specific operations they support, their vulnerability information and other data relevant to assuring the availability of key infrastructure commodities and maintaining port operations. The DCIP database does not duplicate all of the detailed information about assets that may exist in external GIS data sets but is intended to participate in a federated data structure.

To support the assessment teams, DPO-MA developers have created an ArcGIS extension for use at remote sites. This extension, called the Mobile Assessment Extension (MAX) allows assessors to collect much of the needed asset information visually using a map in ArcMap 8.3. The system is deployed on a Tablet PC running Microsoft Windows XP Tablet PC Edition. The system is also equipped with a GPS device and a digital camera. MAX was developed with Microsoft Visual Basic.NET 2003 using object-oriented programming techniques.

The MAX tool populates a Microsoft Access version of the DCIP database structure. This enables relatively easy transformation and loading into the master DCIP database in Oracle. All of the detailed background and infrastructure data collected in earlier phases is loaded onto the Tablet PC to provide a rich cartographic environment in which the assessors may work. The user interface allows for the collection of asset locations in either one of four ways: 1) the user may click on the map to capture an asset location, 2) the user can capture a location from a GPS stream, 3) the user can capture a location by selecting a feature from another vector layer loaded into the ArcMap document, and 4) by typing in the location manually. In the event the user chooses the third method, the location is calculated based on the type of feature selected. If the feature is a polygon, the centroid is captured. For a linear feature, the midpoint is captured. For point features, the point itself is captured. The DCIP database requires that all locations be stored using the World Geodetic System of 1984 (WGS84) geographic coordinate system. Therefore, MAX transforms all coordinates into WGS84 before inserting them into the database.

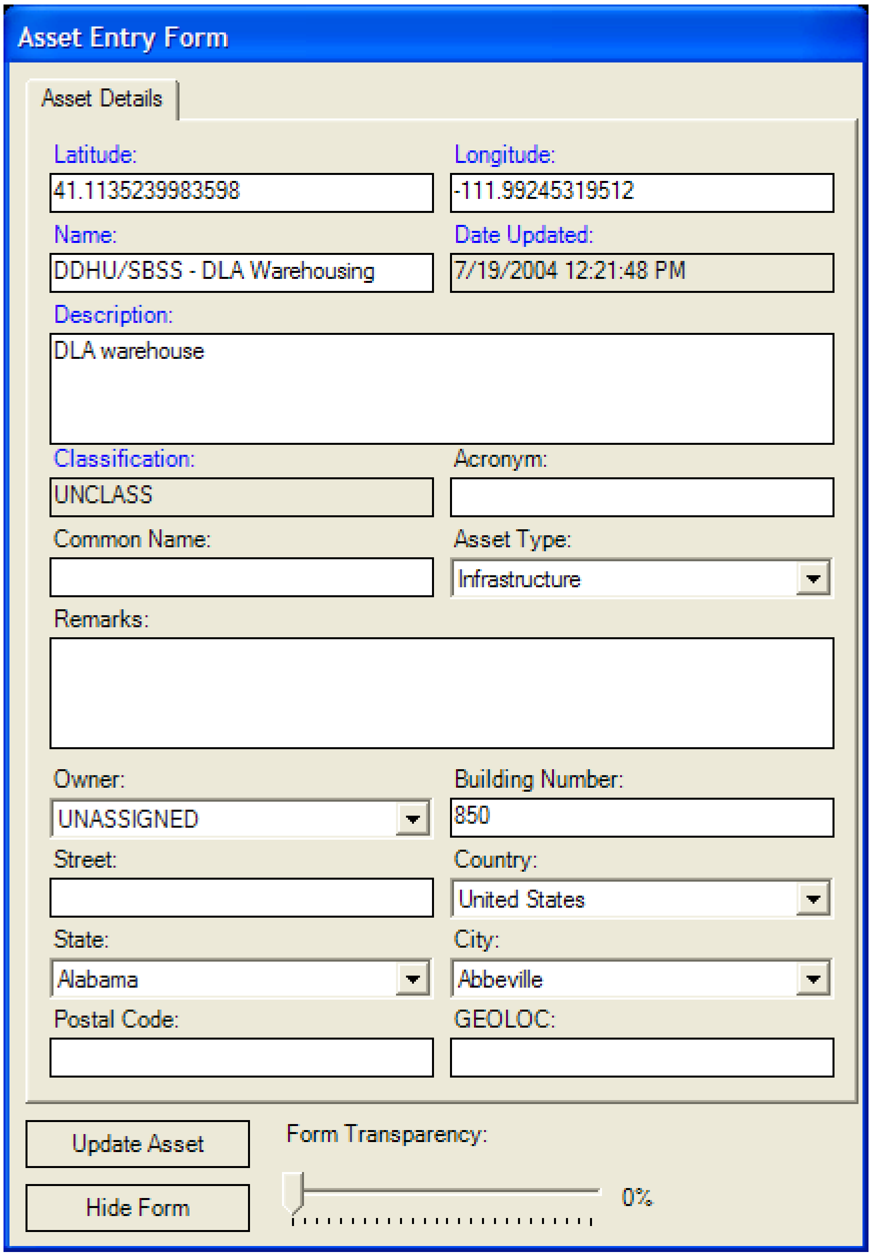

Figure 2: MAX asset entry form with sample data

All of the tools mentioned display a custom form to allow the assessor to capture the other attribute information required by the DCIP database. In addition to asset location, information about relevant points of contact (asset owner, asset manager, etc.), notes and associated files are also collected. Files can include documents such as standard operating procedures and remediation plans as well as digital photos of the asset or key physical features of the asset. All files are stored in the MAX database as binary objects that can be loaded into the master DCIP database.

The introduction of the MAX toolkit to the on-site assessment process has reduced the amount of time dedicated to the processing of information. Prior to MAX, much information was collected on paper or in unstructured spreadsheets and Microsoft Word documents. The GIS interface of ArcMap has proven very popular with assessors and, with training and repetition, they are becoming more comfortable with the MAX tool. MAX is a relatively new tool to the DPO-MA assessment process and is undergoing continuous improvement. Other tools are still used on-site to accomplish other tasks but the long-term goal is to expand MAX to become a single environment for the assessors to use.

The Post-Visit Phase

After the on-site assessment has been completed, the main focus of the assessment team becomes the aggregation and collation of data as well as the creation of the final vulnerability assessment report. The report can contain any number of components, from textual documents to static maps to live, web-based maps. The production of the final report is a labor-intensive process and GIS plays an important role in some areas.

As previously indicated, a large amount of geospatial data related to the port and it supporting infrastructures is collected, created and/or analyzed. Because the final report will contain recommendations about how to minimize identified vulnerabilities and because those recommendations will most likely lead to action, it is crucial the data supporting the recommendations is carefully scrutinized.

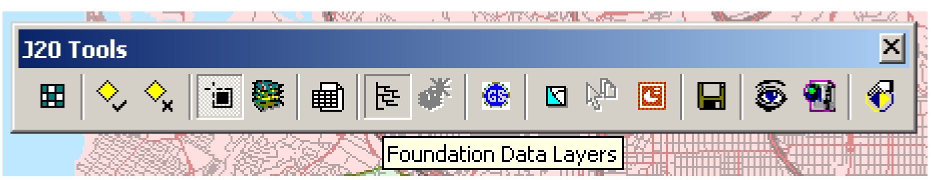

Figure 3: J20 Toolbar provides many custom tools to enhance workflows. Tools are a mix of internally developed tools, ESRI unsupported tools and tools from ArcScripts

With regard to geospatial data sets, many traditional quality assurance practices are followed. Vector layers are aligned with supporting imagery. Topological relationships are verified where appropriate. Attributes are verified based upon information collected on the site visit. In addition, the cartographic integrity of the finished products is verified against internal DPO-MA standards to ensure consistency. For all of these tasks, ArcMap is an indispensable tool. Much of the out-of-the-box capability is leveraged during this time but some custom tools also come into play.

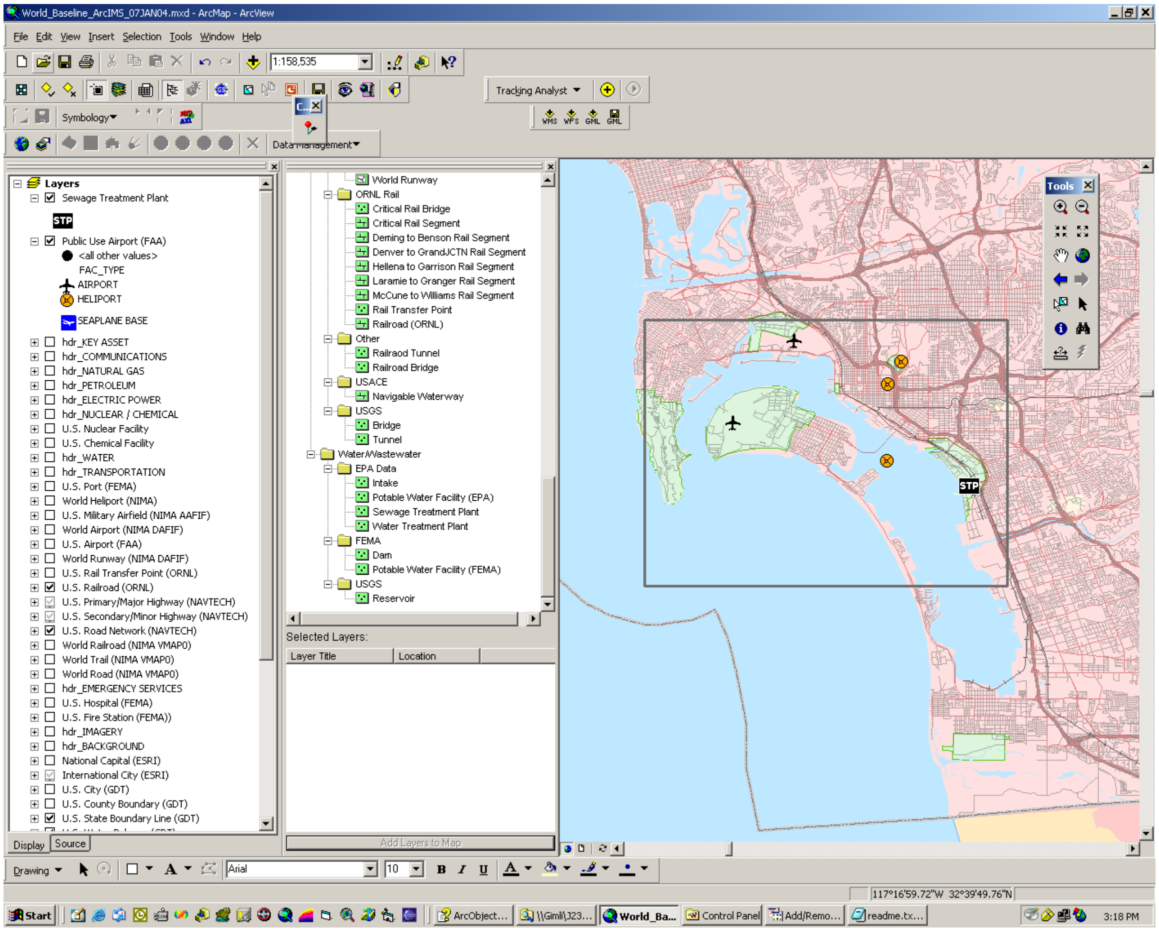

Figure 4: The Foundation Data Tool automatically clips and symbolizes GIS layers for infrastructure analysts

DPO-MA developers have produced a handful of custom tools to streamline production workflows. For example, one tool presents all of the foundation spatial data holdings in a dockable ArcMap window (see Figure 4), with the data sets organized into a hierarchy by functional use (transportation, energy, emergency services, basemap, etc.). Each data set is labeled with a common name that is understood by the analyst community. In this way, many of the usability issues of ArcCatalog have been circumvented. By simply building a list of data sets and then drawing a rectangular area of interest, map layers are created and loaded that contain only the features that fall within the specified area of interest. If a standard symbology set has been defined for a data set, it is applied automatically.

In another case, DPO-MA developers capitalized on a set of code from ArcScripts to create a toolbar that allows an analyst to define symbology for a layer, save the symbol set and load it into another layer later. This differs from the traditional ArcMap layer file because the symbology is divorced from the data set definition. In practice, the tool behaves much like the .avl files used in ArcView 3.x.

Once the data has been verified and final products have been created, they must be made available for dissemination. All DPO-MA products are classified and only made available via classified networks to those with appropriate clearance. The key dissemination environment used is the Homeland Defense Mission Assurance Portal (HD-MAP). HD-MAP is an ArcIMS 4.0.1 based web portal that was developed using Microsoft Active Server Pages (ASP).

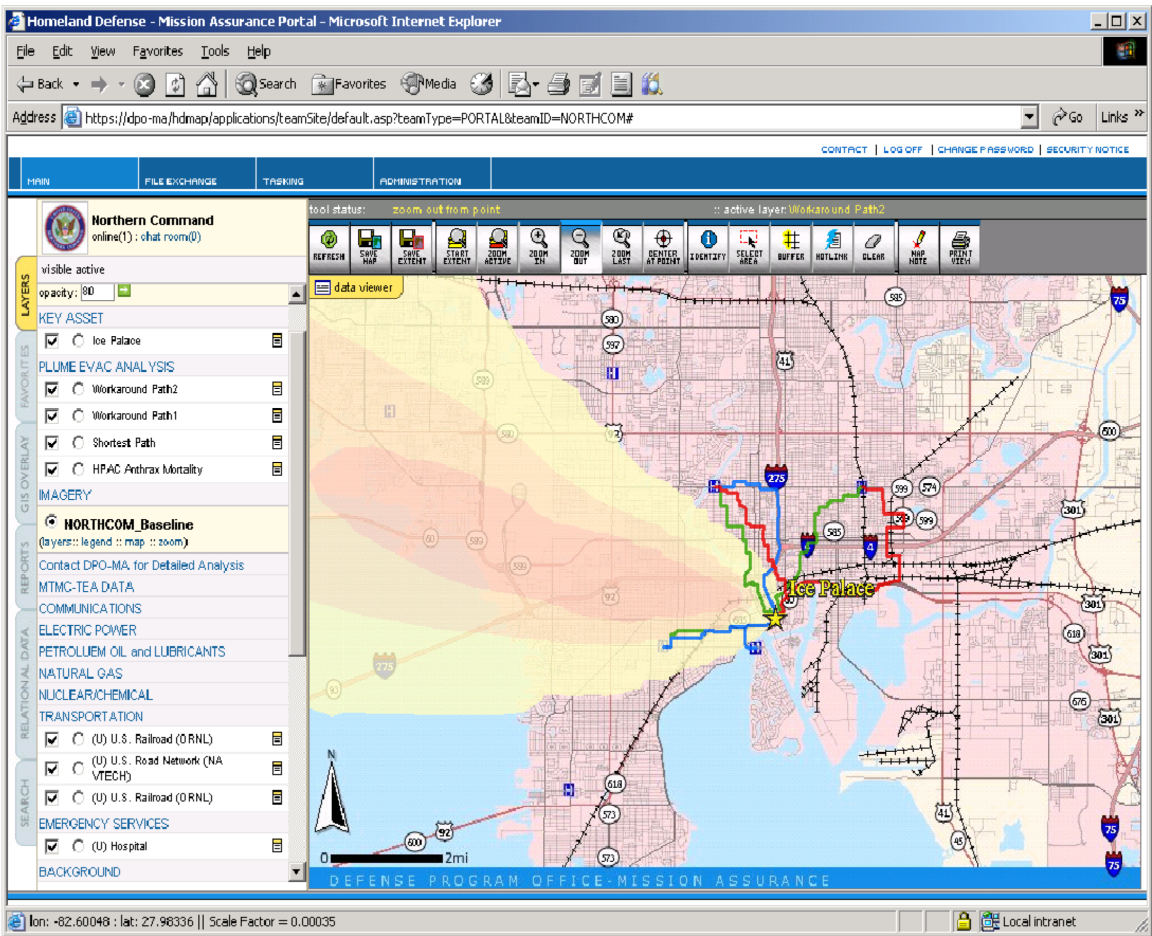

Figure 5: HD-MAP geographic web portal is used to disseminate assessment results.

HD-MAP is a geographic web portal. Whereas many web portals have maps as a component of their interface, HD-MAP leverages geographic context to pare down the list of available content to that which is relevant to the user's current map extent. All products (electronic documents, spreadsheets, geospatial data sets, etc.) are loaded into HD-MAP for dissemination. Those products that are not inherently geospatial are registered to a relevant area of interest. If the user's map extent intersects the area of interest of a product, that product is made available to the user. Because many of the infrastructure and vulnerability assessment products produced by DPO-MA are used in an operational context, this feature has proven useful for presenting relevant information quickly to users.

HD-MAP also possesses collaboration features. First, map notes and hot links are used extensively in the maps. Map notes can be added by any user and become visible to all others who view the same area. Second, a chat feature has been implemented so that currently logged in users may collaborate.

HD-MAP utilizes a "one-map" interface. ArcIMS map services can be layered atop one another, giving the user the ability to create custom maps and also allowing analysts to create more compact map services. Using this approach, there is only one basemap service running. As new services are created, they contain only those layers that are specific to the product. These product-specific services can then be layered over the basemap service and each other to create and custom view of the infrastructure picture in and around a port.

The Department of Defense places extensive restrictions on the use of "mobile code." Mobile code refers to any client-side programming ranging from dynamic HTML scripting to Java applets and ActiveX controls. Essentially, applets and ActiveX controls are not allowed except under the strictest of circumstances. Getting applet-based systems accredited is prohibitively difficult so the HD-MAP features described above could not be implemented using the built-in capabilities of the ArcIMS Java Viewer. As a result, they are all custom implementations.

Future Directions

To support the full range of Defense Critical Infrastructure Program requirements, DPO-MA is striving to produce an integrated, comprehensive situational awareness environment that includes complete maritime domain awareness. To this end, DPO-MA analysts and developers are focusing on the integration of temporally sensitive, dynamic data feeds into the robust ArcGIS environment already in use.

Such feeds include the movement of maritime, air and land-based (road and rail) tracks and well as environmental feeds such as weather and seismic activity. These information feeds are already available across government and industry but they are rarely easily integrated into commercial GIS systems. The ability to integrate such feeds into a comprehensive CIP picture will allow infrastructure analysts to assess the potential impacts of "tracks of interest" on critical infrastructure assets. This capability will enhance the ability to assure key port operations by providing a geographic view of the ever-changing situational environment.

DPO-MA developers have integrated ArcMap with standard DoD situational awareness tools to integrate air and maritime tracks as simple XY event themes but their work is ongoing into the implementation of more sophisticated approaches. Currently, DPO-MA is participating in the ArcGIS Tracking Server beta program to evaluate its ability to meet operational requirements. The ability of ArcGIS Tracking Server to integrate with the advanced analysis capabilities of the ArcGIS Tracking Analyst extension as well as the lifecycle maintenance advantages of COTS software make it an attractive option.

Conclusion

Maritime security requires the consideration of more than shoreline or waterborne threats and vulnerabilities. Ports are complex facilities that depend upon the commodities supplied by supporting infrastructure networks in order to perform their operations. Therefore, a full maritime security picture cannot be built without considering a port's dependencies on supporting infrastructures.

Infrastructure networks and their component assets have an obvious geographic context that is ideally suited for analysis using GIS tools. DPO-MA analysts and developers have long recognized the need for useful, relevant GIS tools to enhance the quality of infrastructure analysis processes. Ultimately, serious infrastructure analysis cannot occur without the inclusion of GIS tools in the process.