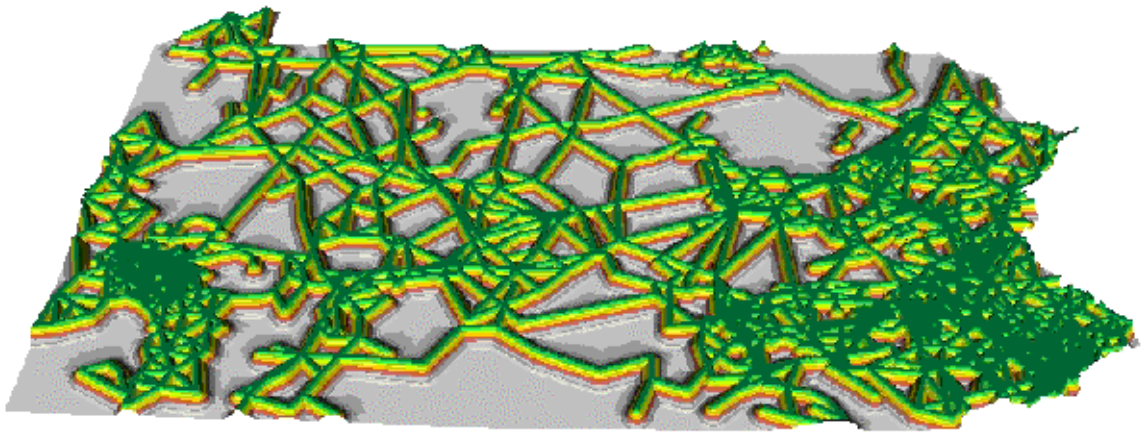
Threat Potential Modeling

Ken Sochats
Director, Visual Information Systems Center (VISC)
School of Information Sciences
University of Pittsburgh
January 8, 2002

This project aims to develop a geo-spatial system that assists security analysts and planners in assessing the risks to infrastructure elements as a result of terrorist attacks.

For the past two years the Visual Information Systems Center has been working on an economic development project for the Commonwealth of Pennsylvania called Technology Opportunity Modeling (TOM). One goal of TOM is to identify and characterize areas of the Commonwealth that possess the necessary resources (financial, technology savvy workforce, information infrastructure, recreational, real estate, etc.) that are conducive to attracting high tech firms. TOM relies on the Pennsylvania Technology Atlas for the identification and location of these resources. Each of these resources is evaluated as to its importance with respect to attracting high tech development and its area of economic impact defined.

The image below models the routes and interconnections of optical fiber communications lines in Pennsylvania. Surrounding each line is a "buffer" area where it is economically and technically feasible to provide high-speed telecommunications services supported by those lines.



All of the resource importance factors are combined for every point in a region using a weighting function to give what effectively we refer to as an "opportunity" index. A high value on the index means that the location has a combination of factors that match well with the typical needs of a high tech firm. When the

indexes are color coded and plotted on a map of the region, the result is a visualization of the relative attractiveness of areas of the region for high tech economic development. TOM has other facilities for deficit analysis, scenario modeling and other type of analyses.

Mapping technological opportunities seems to be not tremendously different from mapping threat potential at a conceptual level.

We propose to adapt the techniques that we developed to model technology opportunity to create a system that provides modeling capabilities for assessing the vulnerability of regions to terrorist attacks. In this system, every important "asset" in a region would be identified and geo-located. These assets would include schools, power companies, telecommunications facilities, businesses, population centers, airports, hospitals, government facilities, storage facilities, reservoirs and any other valuable infrastructure element. Each of these assets would be evaluated as to "value" and impact area. An indexing function would be developed to combine the effects of all the assets into a "Threat Potential" measure. This measure would be color-coded and mapped to show areas of high threat. Functions could be developed to simulate the effects of various terrorist actions (explosions, poisons, crashing, etc.). Other facilities could be developed to analyze various scenarios of attack, security, precautions, interventions, etc.

Some of the reasons for creating a system that models threat potentials are:

Assets might be collocated. Quite often energy transmission, transportation and communication systems share the same right-of-way, intersect or interrelate in some fashion. An attack on one asset at any point may effectively be an attack on all of the assets.

Assets may be proximate. Consequential damage resulting from an attack on an asset may cause damage to a nearby asset. Such was the case with Verizon's central office located near the World Trade Center. Indeed, the concept of proximity is relative. The significance of the Three Mile Island nuclear accident was not the potential destruction of the power plant, but the much greater impact of the subsequent radioactive pollution of all downstream assets.

Security units for these assets are "silo" systems. The power companies, telecommunications companies, transportation companies all have their own security units. In general they do not cooperate or communicate. They may or may not be coordinated with the police or other security force for the local jurisdiction.

Such a system could be used to:

1. Identify areas of high risk.
2. Assist in plans for protecting those assets.
3. Coordinate diverse and disparate security systems.
4. Provide the basis for scenario modeling.
5. Identify information that must be accessed to target those assets.
6. Plan for recovery in the event of attack.