

**Allocation of Resources for Risk Management**  
**Rae Zimmerman, et al, New York University**  
 rae.zimmerman@nyu.edu

1. Overview .....	1
2. Research Accomplishments.....	3
2.1. Modeling the Risks and Consequences of Electricity Outages.....	3
2.2. Infrastructure Resiliency and Vulnerability.....	6
2.2.1. General Concepts.....	6
2.2.2. Oil and Natural Gas .....	6
2.2.3. Transportation Infrastructure .....	8
2.3. Infrastructure Interdependencies.....	9
2.4. Role of Infrastructure in Vulnerability of Special Populations in Catastrophic Events: The Elderly during Natural Hazard Events .....	10
3. Applied Relevance.....	11

**1. Overview**

NYU’s research focused on patterns and trends in critical infrastructure location and disruptions nationwide and the consequences of these disruptions and their implications for potential terrorist attacks and the allocation of resources for risk management. Models that are used to obtain research results are also important transferable decision tools and include applications of negative binomial regression, logistic regression, and weighted least squares regression, linear programming, scenario construction, GIS, and bivariate indicators or ratio techniques. These models were applied to information on resource allocations and the capacity, consumption, and value of infrastructure in combination with characteristics of the location for selected infrastructure areas, such as energy and transportation. In the case of disruptions, disruption causes and consequences were included in the models. Outputs consisted of decision tools and policy implications, as well as research results from applying methods of analysis to infrastructure databases.

Specifically, the models have been used to gain a better understanding of how different initiating causes of infrastructure failures (electric power outages, oil pipeline accidents, and natural gas transmission and distribution pipeline incidents) are associated with consequence measures such as outage duration, customers affected, property damages, and clean-up and recovery costs among others. Earlier results of the modeling upon which this research builds, allow for the construction of scenarios which can be important decision-tools for policy analysts and risk managers in these sectors. For example, in the case of electric power outages the regression models were used to estimate what a potential terrorist attack in New York City would cost. The estimate for an attack on electric power in New York City during Winter was approximately \$1.2 billion. Earlier research developed a number of scenarios for hazardous (petroleum products) liquid pipelines showed that depending on the characteristics of the accident and the initiating cause cleanup and recovery costs can range between \$9,000 and \$46 million. Similar results were obtained for property damage and value of product lost. The results of such scenarios can be important inputs to industry managers and policy analysts as they consider where resources should be put in order to minimize the risk of an accident. A different approach using linear programming was used to estimate the economic costs of a potential terrorist attack on electric power on New Jersey. This work suggests ranges for multipliers that policy makers can use to estimate the likely impacts of electricity outages on other sectors, primarily in terms of time to recover.

A number of other research efforts by the NYU team are relevant for emergency management and security policy. In the case of electric power outage and natural gas and oil pipeline accidents regression

"This research was supported by the United States Department of Homeland Security through the Center for Risk and Economic Analysis of Terrorism Events (CREATE) under grant number 2007-ST-061-000001. However, any opinions, findings, and conclusions or recommendations in this document are those of the authors and do not necessarily reflect views of the United States Department of Homeland Security."

models show important geographical variations in rates of failures at the state level. These analyses can provide inputs to resource allocation efforts that aim to minimize risk of failure. Understanding these spatial variations and the consequence measures associated with failures can also help policy analysts identify areas that would be particularly vulnerable to terrorist attacks.

In an exploratory paper on the policy relevance of the NYU research work titled “Critical Infrastructure Policy for Homeland Security: A Preliminary Summary and Approach” a number of areas were identified where the research could be used as inputs to national security and resource allocation policies. These examples include the following:

#### Urban Area Security Initiative (UASI) Results:

- The NYU bridge and airport infrastructure databases were incorporated into a model in collaboration with CREATE’s partner at the U. of Wisconsin to evaluate the impact of incorporating infrastructure into an attacker model. The results of this collaborative work will allow decision-makers to rank cities and other geographic areas according to the risk of attack given alternative infrastructure attributes as inputs to the model. With these two infrastructure datasets, the ordering of cities according to relative risk changes from one using different criteria that do not incorporate infrastructure.
- As part of NYU’s resource allocation work we have studied the spatial concentration of different infrastructure assets and how current resource allocation by state relates to this distribution of assets. Preliminary findings extended to the city level show that for bridges and airports there is a correlation of roughly 0.5 to 0.6 with FY06 funding levels for a set of ten cities. For other critical infrastructure systems, such as total dam capacity by state, there appears to be little relationship with FY06 funding levels, however at the county level (our current focus) different relationships may appear. This kind of analysis can provide important inputs to and a model for decision-makers working in the area of resource and funding allocation for a variety of different infrastructure types and characteristics.

#### Infrastructure Protection Program (IPP) Fund Results:

- For urban transit, our research found that funds allocated per trip for cities eligible for funding under the Transit Security Grant Program (TSGP) ranged from \$1 to \$8 per transit trip. Comparing these allocations to attributes of the transit infrastructure, in particular, concentration of use, in each of these cities, can guide allocation decisions.
- Water security funding, not directly a part of the IPP funding (though indirectly dealt with under BZPP), was estimated by U.S. GAO to range from \$647,000 to \$13.1 million per plant for conversion from chlorine to other less vulnerable alternatives at selected larger plants. An NYU analysis of the conversion shows a moderately positive correlation between conversion cost and plant size. Further analyses of these data by location and proximate populations and along transport routes for chlorine provide input into policies regarding funding prioritization for conversion and protective boundary alternatives.

NYU’s research work has used incident level information from a number of databases, and each one of these incidents is an actual case or case study. The incident level databases include the Disturbance Analysis Working Group database of 400 electricity outages for the period 1990-2004, three incident databases for the oil and gas sector (hazardous liquid accidents, natural gas transmission and distribution) for the periods 2002-2005 for the first two and 2004-2005 for gas distribution. Hazardous liquid accidents included information about 1,582 incidents, natural gas transmission consists of about 434 incidents, and natural gas distribution consists of 269 incidents for the periods studied. The NYU team also used the

MIPT/Rand databases for infrastructure that is incident-based and covers international attacks of all kinds including electricity, oil and gas, transportation and telecommunications infrastructure. The MIPT database has enabled the team to get down to the asset level in terms of the specific type of component targeted by terrorist attacks.

Efforts that involved collaboration with organizations include work with NYS Assemblymen primarily on electric power outages in the state. Within CREATE, NYU has collaborated with the University of Wisconsin involving resource allocation, and NYU provided infrastructure inputs for their model. ICIS has also shared its work at DHS events, e.g., in March and May of 2007. Collaboration with respect to events included collaborations with other CREATE members for a symposium at the SRA conference in December 2006. ICIS also co-sponsored events with a transportation center at the NYU-Wagner School.

## 2. Research Accomplishments

NYU's fit in CREATE's research framework is primarily in the risk management area, though this work also interfaces with risk assessment and economic assessment. Our resource allocation research advances the science first in identifying and analyzing patterns and trends in infrastructure disruptions in situations analogous to terrorism or from terrorism. Second, it also has identified those factors that contribute to disruption and the consequences of those disruptions as a basis for estimating and forecasting the impacts of future attacks. Third, it associates areas in which infrastructure use or assets are concentrated with DHS allocations as a basis for future allocation priorities.

The models that are used include: Negative binomial regression, logistic regression, and weighted least squares regression models, linear programming, scenario construction, GIS, and bivariate indicators or ratio techniques applied to the capacity, consumption, and value of infrastructure in combination with characteristics of the location, and in the case of disruptions, disruption causes and consequences. Portions of this research have been integrated with the University of Wisconsin's research.

Research results are organized into the following four areas: modeling the risks and consequences of electricity outages; infrastructure resiliency and vulnerability; infrastructure interdependencies; and the role of infrastructure in vulnerability of special populations in catastrophic events: the elderly during natural hazard events. Abstracts of research papers are used to address the research and policy relevance as appropriate.

### 2.1. Modeling the Risks and Consequences of Electricity Outages

Energy infrastructure (including electricity and oil and gas infrastructures) is the driving force behind many other types of infrastructures and activities, and is a frequent target of terrorist attacks. An analysis of the MIPT/Rand database shows that this category has ranked highest or second highest among utility attacks internationally, and exceeds others from 2003 onward. The NYU work in this area has focused on electricity transmission, energy generation, oil transmission and natural gas transmission and distribution facilities.

J.S. Simonoff, C.E. Restrepo, and R. Zimmerman (2007) "Risk Management and Risk Analysis-Based Decision Tools for Attacks on Electric Power," *Risk Analysis*, Vol. 27 (3), pp. 547-570.

Abstract: "Incident data about disruptions to the electric power grid provide useful information that can be used as inputs into risk management policies in the energy sector or disruptions from a variety of origins, including terrorist attacks. This article uses data from the Disturbance Analysis Working Group (DAWG) database, which is maintained by the North American Electric Reliability Council (NERC), to

look at incidents over time in the United States and Canada for the period 1990–2004. Negative binomial regression, logistic regression, and weighted least squares regression are used to gain a better understanding of how these disturbances varied over time and by season during this period, and to analyze how characteristics such as number of customers lost and outage duration are related to different characteristics of the outages. The results of the models can be used as inputs to construct various scenarios to estimate potential outcomes of electric power outages, encompassing the risks, consequences, and costs of such outages.” The approach and statistical models used to analyze electric power outages constitute a tool that can be applied to other critical infrastructure incident analyses.

**Policy relevance:** The relevance of this work to homeland security policy is to be able to identify the consequences of electricity disruption as a basis for developing policies to identify which electricity facilities and locations should be prioritized on the basis of where adverse consequences are greatest and identify mitigation measures that focus on the causes of such events.

R. Zimmerman, C.E. Restrepo, J.S. Simonoff, and L. Lave (2007) “Risk and Economic Cost of a Terrorist Attack on the Electric System,” Chapter 14 in *The Economic Costs and Consequences of Terrorism*, edited by H.W. Richardson, P. Gordon and J.E. Moore II. Cheltenham, UK: Edward Elgar Publishers, pp. 273-290.

This book chapter describes a methodology and approach developed by the research team to use the outputs of the statistical regression modeling work on electric power outages to estimate the potential economic costs associated with a terrorist attack on the electricity infrastructure. The economic cost accounting approach uses three major categories: business losses associated with lost economic activity for the population affected, economic costs associated with injuries and fatalities resulting from a power outage, and economic costs associated with increased traffic congestion. The regression models provide outputs such as duration and number of customers lost during an outage by different cause. The methodology is applied to a scenario of a potential terrorist attack on electric power in New York City during the winter. Crime was used as a proxy for the cause of the power outage in the regression model and the results suggest an outage duration of approximately 20 hours and about 900,000 customers lost (each customer is assumed to be the equivalent of three people affected in the calculation). The scenario also assumes 150 fatalities resulting from the power outage. Such fatalities could be due to problems in the provision of health services during an outage. In addition, four hours of extra delays related to transportation congestion are included in the estimate. The total cost of such an outage is estimated to be approximately \$1.2 billion. This approach and methodology can be used for scenario construction in other geographical areas to provide inputs to risk management when quick calculations about cost estimates are needed.

**Policy relevance:** Policy analysts can use this approach to evaluate the approximate costs of alternative characteristics of energy disruption.

M.R. Greenberg and R. Zimmerman (forthcoming, accepted for publication) “Distribution of federal anti-terrorism funds in the United States: a comparison of data-driven approaches based on electric power generation,” in *Terrorism Issues: Threat Assessment, Consequences and Prevention*, edited by F. Columbus. Hauppauge, NY: Nova Science Publishers, Inc.

M. R. Greenberg, W. Irving, and R. Zimmerman, “A Screening Model for Allocating Department of Homeland Security Funds to Local Governments and States with Explicit Equity, Population and Need Criteria.”

This book chapter and manuscript have as their objectives or targeted problems to compare the geographical distribution of Department of Homeland Security (DHS) funds to states and local governments to a synthetic distribution that explicitly addresses political equity, population size, and the geographical location of electricity generating capacity.

The databases used are county and state level population, land area, electricity generation, location of nuclear power plants, and retail price of electricity (the book chapter focuses only on the state level). These factors are surrogates for other characteristics as described below.

Approaches/methods (transferable tools): The NYU research uses a linear programming model. The objective function maximizes funds allocated based on the distribution of electricity generation (surrogate for infrastructure), retail price of electricity (surrogate for value of electricity), land area (surrogate for area that needs to be protected by state/local government), and presence of nuclear power plants (surrogate for risk perception and consequences). Combinations of the objective function are tried. Constraints are: set aside for political equity (minimum amount each state) and population size; and ceilings on amount of funds to any single county. (See attachment for equations.)

Findings: Set-asides are systematically varied to determine the impact on the geographical distribution of funds. Populous states like California, New York, Texas, Florida, and Illinois receive a good deal of funding under all the scenarios because all of their electricity generation and population size. When political equity set-aside increases, however, funds are drawn away from North Carolina, South Carolina, Indiana and several other states that generate a disproportionate amount of electricity, but are not among the most populated states. With regard to the comparison with Department of Homeland Security allocations to states and local governments, the combination of electrical generation x retail price per kilowatt hour in the objective function, along with 60% allocated for political equity and population size, and a ceiling of \$50 million for maximum county allocation is a good approximation of the DHS distributions for fiscal year 2006 and fiscal year 2007.

Policy relevance: This model can be used by the Department to simulate likely distributions of funds given different kinds of infrastructure, and different levels of emphasis on set-asides for population size and political equity. The model is very simple to use, and is able to incorporate already published data, as well as more detailed information.

M. Greenberg, N. Mantell, M. Lahr, F. Felder, and R. Zimmerman (2007) "Short and Intermediate Economic Impacts of a Terrorist-Initiated Loss of Electric Power: Case Study of New Jersey," *Energy Policy*, Vol. 35 (1), pp. 722-733.

Abstract: "The economic impacts of potential terrorist attacks on the New Jersey electric power system are examined using a regional econometric model. The magnitude and duration of the effects vary by type of business and income measure. We assume damage is done during in the summer 2005 quarter, a peak period for energy use. The state economy recovers within a year, if we assume that economic activity is restored in the next time period. However, if the attacks prompt an absolute of loss of activity due to firm relocation, closing, and geographical changes in expansion plans, then the economy does not fully recover by the year 2010. Hence, the electrical power system's resiliency to damage is the key to the extent and duration of any economic consequences of a terrorist attack, at least in New Jersey."

Policy relevance: "The policy implication is that the costs and benefits of making the electric power system more resilient to plausible attacks should be weighed and that the restorative capacity of the system should be strengthened."

## 2.2. Infrastructure Resiliency and Vulnerability

### 2.2.1. General Concepts

R. Zimmerman (forthcoming and in press 2007) “Managing Infrastructure Resiliency, Safety and Security,” in *Encyclopedia of Quantitative Risk Assessment*, edited by B. Everitt and E. Melnick. New York, NY: John Wiley.

Abstract. “Infrastructure reliability in its most general sense refers to whether a system performs as expected. Reliability is relative, depending on the perspective of the infrastructure user. Safety and security are key components for the concept of reliability, since they pertain to basic survival, and are prerequisites for others. Safety and security are defined, and their emergence as core concepts in infrastructure reliability is described. Infrastructure security now relates to a set of critical infrastructures. Factors that potentially compromise infrastructure security include how infrastructure is spatially distributed and interrelated or interdependent with other infrastructures. Risk-based analytical approaches, and alternatives to these approaches, have arisen to address the likelihood and form of attacks as well as the consequences of attacks on infrastructure. Selected examples of these methodologies are presented. Resource allocation at the federal level emphasizes a risk-based approach, though the nature of risks faced by critical infrastructures, how these risks should be quantified, what analytical tools should be used to produce such estimates, at what geographic scale, and how they are to be incorporated into prioritization schemes is still a subject of considerable debate.”

Policy relevance: This work identifies how safety, security and reliability can be integrated into the design and planning of infrastructure and the implications of not doing so.

### 2.2.2. Oil and Natural Gas

#### 2.2.2.1. Vulnerabilities in the Oil and Natural Gas Sectors

ICIS has conducted a number of analytical studies on oil and natural gas pipeline failures. The first part of this research consisted in describing and analyzing some important vulnerabilities in the oil and natural gas sectors. This work is summarized in a paper titled “Vulnerabilities in the Oil and Natural Gas Sectors” (currently under review by the *CIP Journal*). The first part of the paper includes an analysis of international terrorist attacks on the oil and natural gas sectors using a database maintained by the National Memorial Institute for the Prevention of Terrorism (MIPT) for the period 1990-2005. Number of attacks, fatalities and injuries were analyzed for countries with the largest number of attacks, including Iraq, Colombia, Pakistan, Russia and others. Although attacks against the oil and natural gas infrastructures are relatively small as a percentage of total terrorist attacks, the incidents show that these sectors are vulnerable. In several countries the number of attacks increased during this period. The data also show that the most frequently targeted components during this period were distribution pipelines (about 70%) and production facilities (primarily refineries, about 15%). These components can also be considered to be the most vulnerable.

The second type of vulnerability analyzed in the paper is accidents and incidents in the U.S. oil and natural gas pipeline networks. Three databases maintained by the U.S. Department of Transportation’s Office of Pipeline Safety (OPS) were analyzed to gain a better understanding of the spatial and temporal distribution of these failures, as well as the consequences associated with them. The types of consequences examined include property damages, product loss, fatalities and injuries. The three

databases included in the analyses are: (i) Hazardous liquid pipeline accidents; (ii) natural gas transmission pipeline incidents; and (iii) natural gas distribution pipeline incidents.

The paper ends with a general discussion of vulnerabilities in the oil and natural gas sectors posed by the reliance on process control systems such as Supervisory Control and Data Acquisition (SCADA) systems to operate and monitor these infrastructure systems. Information from cases and published reports is provided and future research directions in this area are explored. The analyses included in the paper to illustrate important vulnerabilities in this sector can be used as inputs to risk management and infrastructure policies.

Policy relevance: The exploratory analyses of oil and gas data on international attacks and domestic incidents offers important information to risk managers and policy analysts about the types of components that are more likely to fail, incident trends, and causes of failure. More detailed analyses of some of the databases described in this paper were carried out by the ICIS team and are described in the papers summarized below.

#### **2.2.2.2. Spatial and Temporal Analyses**

Spatial and Temporal Analyses of Electrical Power and Oil and Natural Gas Pipeline Failures (to appear in *Critical Infrastructure Protection: Issues and Solutions*, edited by E.D. Goetz and S. Sheno. New York, NY: Springer).

In a paper titled “Analysis of Electrical Power and Oil and Gas Pipeline Failures” we summarize additional work on the spatial and temporal distribution of infrastructure failures. A first general finding of the paper is that overall federally-declared hazards have been increasing at 2.7% per year. In the rest of the paper we examine failures in two critical infrastructure areas. First we looked at electricity failures using data provided by the North American Electric Reliability Council (NERC) through their Disturbance Analysis Working Group (DAWG) database. The period of analysis is 1990-2004 and the database includes information on 400 outages. Geographic Information Systems (GIS) and Poisson regression were used to analyze the spatial distribution of electricity outages at the state level. The data were normalized by the amount of overhead transmission lines in each state so that the variable modeled was outage rates. The results show statistically significant variations in outage rates at the state level with California, North Carolina, New York, Oregon, Florida, Maryland and Michigan having higher than expected outages. Temporal trends in outages were also modeled and the results of the research suggest there was roughly an 8.5% annual increase in outages.

A similar analysis was done for oil and natural gas pipeline failures using data from the Office of Pipeline Safety (OPS). The same databases mentioned in the first paper were used in these analyses. For the hazardous liquid pipelines (which carry products such as oil and other petroleum-derived fuels) the period of analysis was 2002-2005. A Poisson regression model for the number of accidents per 10,000 miles of pipeline at the state level showed there are important variations in the spatial distribution of these accidents. Some of the states with higher than expected pipeline incidents per 10,000 miles of pipeline include California, Delaware, Hawaii, Kansas, Massachusetts, New Jersey and Oklahoma. The analysis of the temporal distribution of pipeline failures suggests that there is a roughly 9% annual decrease in incidents per 10,000 miles of pipeline. Natural gas transmission and distribution pipeline incidents also show statistically significant variations at the state level. In terms of the temporal distribution of the natural gas pipeline incidents, the analyses show that for natural gas transmission pipeline incidents there is a significant temporal increase when offshore incidents that took place on Federal waters without a state designation are included but not when these are excluded. For natural gas distribution incidents there is no evidence of a temporal trend.

Policy relevance: The models presented in this paper constitute tools that can be used by industry analysts, decision analysts, and policy makers to identify trends and vulnerabilities in geographical areas. They can also be used as inputs to resource allocation and risk management policies aimed at reducing the incidence of failure rates in these critical infrastructure systems.

### **2.2.2.3. Causes, Consequences, and Risk Policy Implications of Accidents in U.S. Hazardous Liquid Pipeline Infrastructure**

The most detailed statistical analysis carried out by the ICIS team is for hazardous liquid pipeline accidents. This work is summarized in a paper submitted to the journal *Growth & Change* titled “Causes, Consequences, and Risk Policy Implications of Accidents in U.S. Hazardous Liquid Pipeline Infrastructure.” This work follows a similar approach to earlier analytical work done by the ICIS research team in the electricity sector. That work was summarized in a paper titled “Risk-Management and Risk-Analysis-Based Decision Tools for Attacks on Electric Power” published in the journal *Risk Analysis* described in this section of the report.

In our analysis of hazardous liquid pipeline accidents we use data maintained by the Office of Pipeline Safety (OPS) for the period 2002-2005 to gain a better understanding of the association between different accident causes (such as external corrosion, third party excavation, equipment malfunction, ground movement, fire and others) and consequence measures (such as product loss, call for an evacuation and property damage). During this period of analysis there were 1,582 hazardous liquid pipeline accidents. The first part of the analysis used logistic regression models to understand factors associated with nonzero product loss cost, nonzero property damage cost and nonzero cleanup and recovery costs. In the second part of the analysis least-squares and weighted least-squares regression models were used to understand how factors such as system part involved in the accident, location characteristics (offshore versus onshore location, occurrence in a high consequence area), and whether there was liquid ignition, an explosion, and/or a liquid spill are associated with the magnitude of consequence measures such as property damages, product loss, and cleanup and recovery costs.

In the third part of the analysis the results of the regression models are applied to hypothetical scenarios for hazardous pipeline accidents. The results of the scenarios are used to illustrate how variables such as property damage and cleanup and recovery costs depend on the initiating cause of the accident and the other factors examined.

Policy relevance: The models used in this research constitute an analytical decision-tool that can be applied to prioritize resource allocation and to guide risk management. Both industry and policy makers can use such a tool to create various scenarios and conduct sensitivity analyses related to the magnitude of different consequence measures that can be expected from different accident characteristics. In the absence of domestic terrorist attack information, these models can also be used to provide estimates of consequence measures for a potential terrorist attack. The NYU team used this approach to estimate the economic costs of a potential terrorist attack on the electric power sector. A similar process of creating scenarios and estimating various categories of economic costs could also be carried out by policy makers and risk managers in the oil and natural gas sector.

### **2.2.3. Transportation Infrastructure**

V. Bier, N. Haphuriwat, J. Menoyo (U. Wisconsin), R. Zimmerman and A. Culpen (NYU), “Optimal Resource Allocation for Multiple Targets,” *Risk Analysis* (submitted July 2007).

Abstract: “This paper describes the results of applying a rigorous computational model to the problem of the optimal defensive resource allocation among potential terrorist targets. In particular, our study explores how the optimal budget allocation depends on the cost effectiveness of security investments, the defender’s valuations of the various targets, and the extent of the defender’s uncertainty about the attacker’s target valuations. We use expected property damage, expected fatalities, and two metrics of critical infrastructure (airports and bridges) as our measures of target attractiveness.”

Policy relevance: “Our results show that the cost effectiveness of security investment has a large impact on the optimal budget allocation. Also, different measures of target attractiveness yield different optimal budget allocations, emphasizing the importance of developing more realistic terrorist objective functions for use in budget allocation decisions for homeland security.”

### 2.3. Infrastructure Interdependencies

A set of papers develops methods of measuring or estimating dependencies among infrastructures.

Policy relevance: Given a particular type of infrastructure, policy makers can understand the likelihood of repercussions of failures in other infrastructures upon which the given type of infrastructure is dependent to inform resource allocation choices.

R. Zimmerman, “Understanding the Implications of Critical Infrastructure Interdependencies,” Wiley Handbook of Science and Technology for Homeland Security. John Wiley & Sons, Inc. (submitted July 2007; Under Review).

This work focuses on the water sector and the types of infrastructure that influence it and upon which water is dependent. Examples of rates of use of other infrastructure services are given as a guide to estimating impacts.

R. Zimmerman and C.E. Restrepo (2006) “The Next Step: Quantifying Infrastructure Interdependencies to Improve Security,” *International Journal of Critical Infrastructures*, Vol. 2 (2/3), pp. 215-230.

Abstract: “Understanding cascading effects among interdependent infrastructure systems can have an important effect on public policies that aim to address vulnerabilities in critical infrastructures, especially those policies pertaining to infrastructure security. Efforts to quantify these cascading effects and illustrative examples of such metrics are presented. The first set of examples is based upon various impacts that the 14th August, 2003 blackout in the USA had on other sectors. A second set of examples is based on various electric power outages and their impact on other infrastructure systems collected from the authors’ research. Although efforts to quantify cascading effects are challenging, given the nature of the data and its limited availability, research in this area can provide useful metrics.”

Policy relevance: This work suggests ranges for multipliers that policy makers can use to estimate the likely impacts of electricity outages on other sectors, primarily in terms of time to recover. This contributes to resource allocation criteria.

C.E. Restrepo, J.S. Simonoff, and R. Zimmerman (2006) “Unraveling Geographic Interdependencies in Electric Power Infrastructure,” *Proceedings of the Hawai’i International Conference on System Sciences*, IEEE Computer Society.

Abstract: “Interdependencies among infrastructure systems are now becoming commonplace, and present both opportunities and vulnerabilities. Initial attention was paid to functional interdependencies among infrastructure systems regardless of locational characteristics. Using electric power as a focal point, geographic interdependencies are evaluated, that is, outages that spread across several states rather than being confined to single states. The analysis evaluates the extent to which the two different groups have distinct characteristics. The characteristics examined include incident counts, number of customers lost, duration and energy unserved. Data are drawn from the Disturbance Analysis Working Group (DAWG) database, which is maintained by the North American Electric Reliability Council (NERC), and from the U.S. Energy Information Administration (EIA).”

Policy relevance: The analyses presented in this paper provide policy makers and risk managers with a framework for starting to think about potential geographical interdependencies in infrastructure systems such as electricity. This issue will be particularly relevant in the future as the country’s infrastructure systems become increasingly interconnected with international infrastructure networks.

#### **2.4. Role of Infrastructure in Vulnerability of Special Populations in Catastrophic Events: The Elderly during Natural Hazard Events**

Another area of research pursued by the ICIS team is the vulnerability of particular groups to natural hazard events. In a paper prepared for the Hazards and Disasters Researchers Meeting, held in Boulder, Colorado in July 2007, we explored issues related to potential vulnerabilities to the elderly population by natural hazards. The elderly population is considered to be those aged 65 years and older. A review of the literature indicates that the elderly tend to be more vulnerable due to below-average income levels and more limited mobility. We use Geographic Information Systems (GIS) to analyze the spatial distribution of the elderly population in the United States at the county level, looking at both total numbers of people aged 65 and over and the elderly population as a percentage of the total population.

In addition, we discuss using two databases to identify counties that could be targeted for risk management purposes since they may represent areas of high vulnerability. The first database used was the Spatial Hazard Events and Losses Database, which is maintained by the University of South Carolina’s Hazards & Vulnerability Research Institute. This database contains information about natural hazards events. We looked specifically at the counties with the highest frequency of hurricanes between 1995 and 2005 and matched the data to the elderly population data. During this period FEMA recorded hurricanes and tropical storms in 471 counties (or about 15% of all counties) which had at least one event, and these counties are concentrated in 17 states and DC. Counties in only 4 states – Florida, North Carolina, Alabama, and Louisiana – have had ten or more events from 1995-2005. We also used the Social Vulnerability Index (SoVI), also maintained by the University of South Carolina’s Hazards & Vulnerability Research Institute to provide another measure of vulnerability to the counties with the highest hurricane frequency. Although there are important differences in the number and percentage of elderly in the counties with the highest hurricane frequencies, as well as in the SoVI figures, it is clear that various counties in the states of Florida and North Carolina have high figures for all the variables of interest. These counties are included in a table in the paper.

Policy relevance: This research could provide important inputs into efforts to distribute resources to minimize risks for vulnerable populations such as the elderly by identifying geographical areas such as counties that have important numbers of elderly people with a high vulnerability index. This work is also relevant to policy makers working in the emergency management area.

### 3. Applied Relevance

NYU's research work has used incident level information from a number of databases, and each one of these incidents is an actual case and can be thought of as a case study. In the case of electricity we worked with the Disturbance Analysis Working Group database on electricity outages for the period 1990-2004. The portion of that database analyzed included information on 400 incidents. In the case of the oil and gas sector, the NYU team analyzed three incident databases maintained by the U.S. Department of Transportation's Office of Pipeline Safety (OPS). The three databases are: natural gas transmission incidents (2002-2005), natural gas distribution incidents (2004-2005) and hazardous liquid accidents (2002-2005). For natural gas transmission incidents NYU's analyses focused on data for the period 2002-2005, and the dataset consisted of information about 434 incidents. For natural gas distribution incidents the period 2004-2005 was used and the dataset included information about 269 incidents. For hazardous liquid accidents data for the period 2002-2005 was used, which included information about 1,582 incidents. Finally, the NYU team used the MIPT/Rand database that is incident-based and covers international attacks of all kinds including electricity, oil and gas, transportation and telecommunications infrastructure. The MIPT database has enabled the team to get down to the asset level in terms of the specific type of component targeted.

The NYU team developed an extensive array of databases and decision tools for assessing infrastructure locations, concentration and trends in assets, disruptions, and attacks. The tools have application in risk assessment, economic assessment and risk management, and are intended for risk and economic analysts, utilities, emergency managers, and policy makers. Many of the databases are already fairly complete, though some are under construction, providing a wealth of information on location of facilities, capacity and usage of infrastructure, including transportation and energy. These are available through CREATE's Risk Analysis Workbench (RAW).