DIAGNOSTIC TOOLS TO ESTIMATE CONSEQUENCES OF TERRORISM ATTACKS AGAINST CRITICAL INFRASTRUCTURE

Rae Zimmerman, Carlos Restrepo, Nicole Dooskin, Jeremy Fraissinet, Ray Hartwell, Justin Miller and Wendy Remington[*]

Institute for Civil Infrastructure Systems (ICIS)
Robert F. Wagner Graduate School of Public Service
New York University
295 Lafayette Street
New York, NY 10012
rae.zimmerman@nyu.edu, cer202@nyu.edu, njd229@nyu.edu, jf1220@nyu.edu,
rvh208@nyu.edu, justin.miller@nyu.edu, wer1@nyu.edu

ABSTRACT

Diagnosing historical incidents of terrorism events within a risk management framework is an important tool for understanding the likelihood and form of future terrorist attacks and their consequences, particularly for critical infrastructure. Critical infrastructure is a key potential terrorism target, and government concerns are reflected in numerous laws and documents on critical infrastructure protection. Given the lack of historical precedent for infrastructure attacks in the U.S., other approaches to estimate consequences of attacks are needed to fill a critical knowledge gap. Using electric power as an example, databases of selected terrorist attacks on electric power infrastructure worldwide are evaluated to infer potential consequences of such attacks against U.S. electric power infrastructure. The focus is on electric power system components that are attacked, and consequences of outages from interdependencies with other infrastructure. In addition to analytical results, this work suggests a framework for a tool for decision-makers.

INTRODUCTION

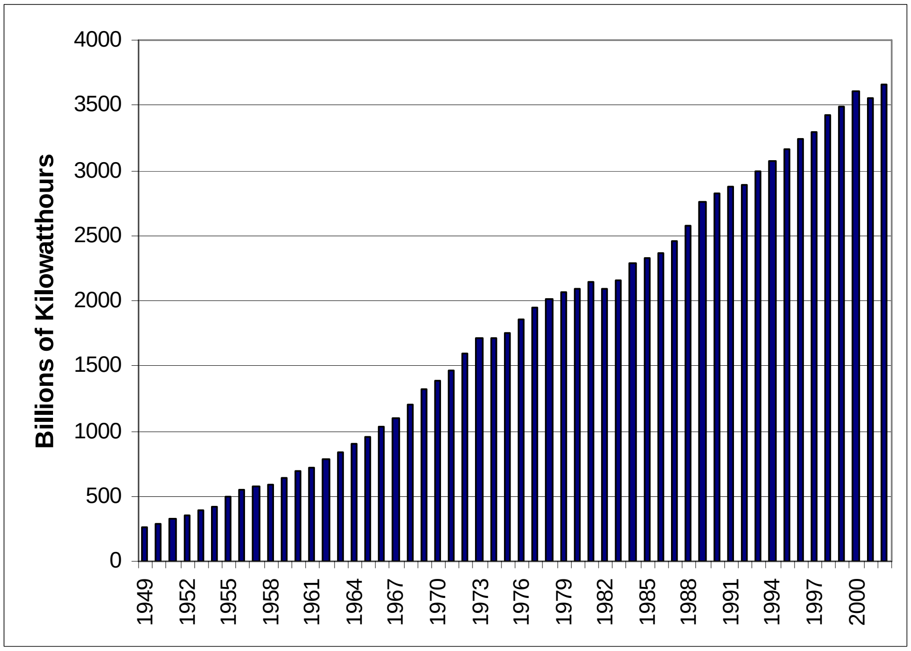
Electricity is a critical infrastructure that is intricately related to all aspects of the U.S. economy and is crucial to the functioning of other infrastructure systems such as transportation, water supply, environmental services, and telecommunications. As Figure 1 shows, over the last five decades through 2002, electricity use in the United States has increased 14-fold from about 255 billion kilowatt-hours to about 3,600 billion kilowatt-hours. By comparison, the total population of the country did not even double, increasing from 152,271,000 in 1950 to 282,434,000 in 2000 [6].

[*] Acknowledgement and Disclaimer: This research was supported by the United States Department of Homeland Security through the Center for Risk and Economic Analysis of Terrorism Events (CREATE), grant number EMW-2004-GR-0112. However, any opinions, findings, and conclusions or recommendations in this document are those of the author (s) and do not necessarily reflect views of the U.S. Department of Homeland Security.

Interruptions in electricity in the form of intermittent outages have accompanied the dramatic rise in the consumption of electricity, and interdependencies between the electricity sector and others have exacerbated the effect of outages. This paper focuses on ongoing research to portray risk elements associated with vulnerabilities in the electricity sector that tend to be associated with outages as a basis for estimating consequences and economic costs of potential attacks against the sector. The overall research methodology is based on scenarios, statistical analyses of events databases, and cost factors derived from impacts of analogous events.

The electricity sector analysis section consists of three parts. The first part portrays potential risks and vulnerabilities to the electricity system in terms of alternative ways in which the electric power system can become disrupted; this information was obtained using events databases to understand ways in which such disruptions have actually occurred in the past. Potential risks and vulnerabilities in the electric power sector in the United States are described by examining domestic electric outage incidents from non-terrorist causes as well as terrorist attacks against electric utilities in other countries. Part two describes efforts to quantify the consequences of electricity outages to other infrastructure sectors. Part three describes how the data examined in the first two sections can be used to estimate economic costs associated with various scenarios that describe potential attacks to the electricity sector. Finally, a concluding section addresses some of the uses of the approach.

Figure 1. Electricity Consumption in the United States: 1949-2002



Source: Graphed from Energy Information Administration (EIA), U.S. Department of Energy, Annual Energy Review 2001, Energy Perspectives: Trends and Milestones 1949-2001.

ELECTRICITY SECTOR ANALYSIS

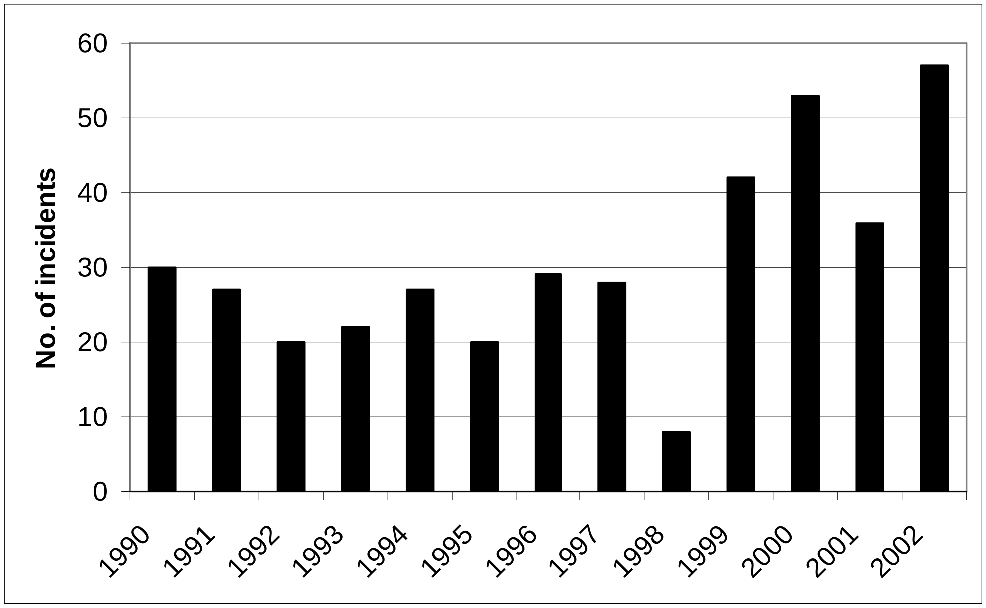
Portraying Risk Elements Associated with the Electricity Sector

Risks to the electricity system are in part reflected in the way electricity has been disrupted in the past. Two kinds of event databases are used to identify how disruptions in electricity have occurred. One is North American and the other is international (other than North American). These databases are being used in two ways to characterize vulnerability. One is for a statistically-based vulnerability assessment. Another is to identify critical components in the electric power systems that tend to be disrupted in an outage.

Trends in Electric Power Outages for Vulnerability Analysis

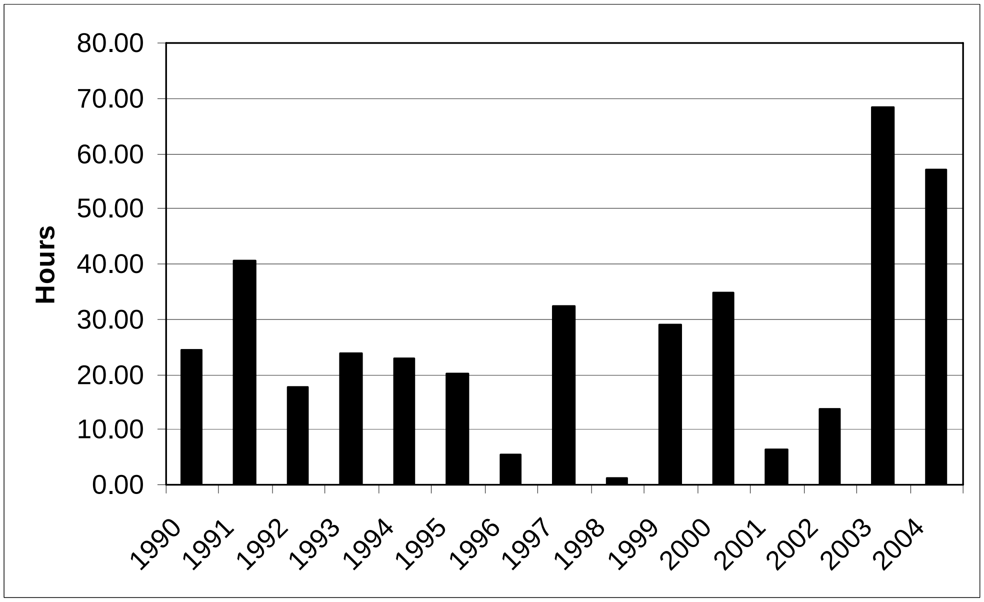
Electric power outages from non-terrorist causes provides a basis for analyzing vulnerability. Information about electric outages in North America is available as part of the North American Electric Reliability Council's (NERC) DAWG database. This includes information about the cause of the outage, components affected, number of customers affected, duration of the incident, and megawatts lost, among other characteristics. Information from the events included in this database was first analyzed to identify time series trends for the variables mentioned above between 1990 and 2002. The yearly averages for number of outages (incidents), customers affected, average incident duration and megawatts lost are summarized in figures 2-5, which include all events in the United States and Canada for which the relevant information was available.

Figure 2. Number of Incidents of Electric Power Outages in the U.S. and Canada: 1990-2002



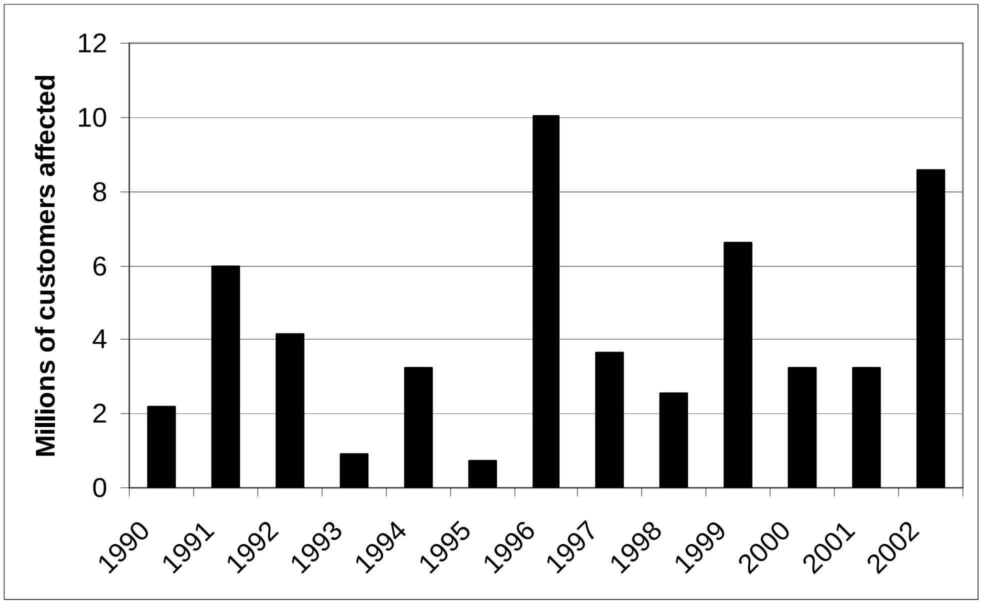
Source: Graphed from data extracted from the North American Electric Reliability Council's (NERC) DAWG database.

Figure 3. Average Duration of Electric Power Outages in the U.S. and Canada: 1990-2002



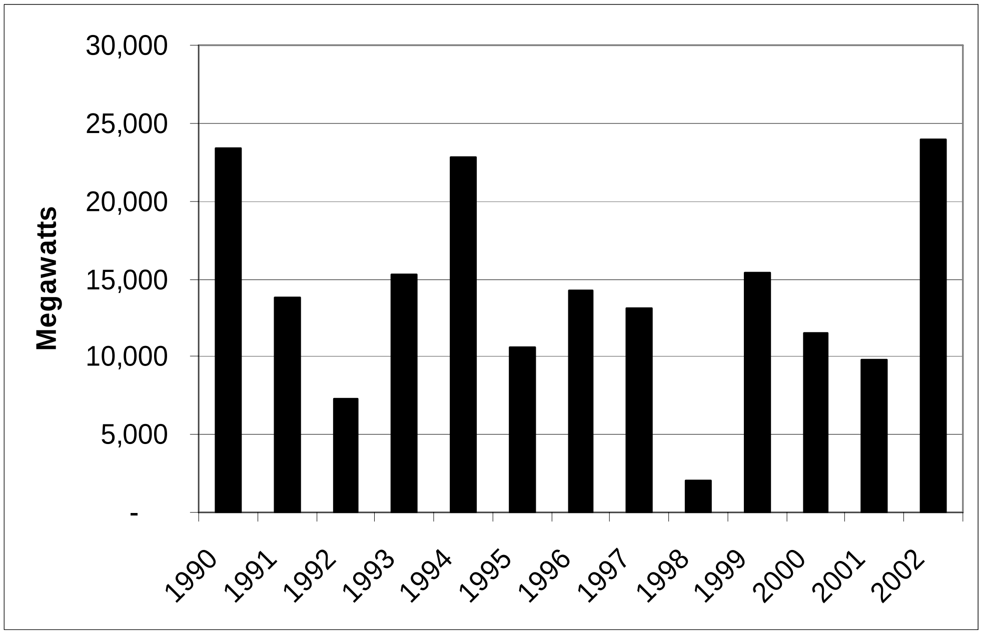
Source: Graphed from data extracted from the North American Electric Reliability Council's (NERC) DAWG database.

Figure 4. Average Number of Customers Affected per Electric Power Outage in the U.S. and Canada: 1990-2002



Source: Graphed from data extracted from the North American Electric Reliability Council's (NERC) DAWG database.

Figure 5. Average Megawatts of Demand Lost per Electric Power Outage in the U.S. and Canada: 1990-2002



Source: Graphed from data extracted from the North American Electric Reliability Council's (NERC) DAWG database.

The graphs only give a very general picture of trends. A preliminary analysis of the data shows that events, duration and number of customers have been increasing since 1990, but the trend in megawatts lost is unclear and appears to be decreasing. The trends are difficult to interpret because of variability in the data. This variability is not surprising given that a large number of these incidents are caused by weather related events, which show much variability from one year to another. For the United States data, about half of the outages were caused by weather between 1990 and 2004. The second biggest cause of outages was equipment failures, which accounted for almost a quarter of the incidents. An analysis by Apt [1] using data from 1984 – 2000 found a similar distribution of events by cause.

A next step in the research project will be to conduct least-squares and negative binomial regressions to examine the associations between these variables for all events for which data is available as a basis for predicting very broadly-based consequences of outages in terms of numbers of customers affected and other characteristics of the electric power systems. For example, these analyses will provide estimates of the effect of variables such as duration of an outage and megawatts of demand lost on number of customers affected for different causes. The causes were categorized to include weather, equipment failures, human error, fires, crime and sabotage, capacity shortages, demand reduction, and others based on the NERC database. Understanding how these different causes affect the nature of outages will allow the project to better estimate the potential impacts of a terrorist attack on the sector since some causes will be more relevant to terrorist attacks than others.

Critical Electric Power Components Disrupted in Outages

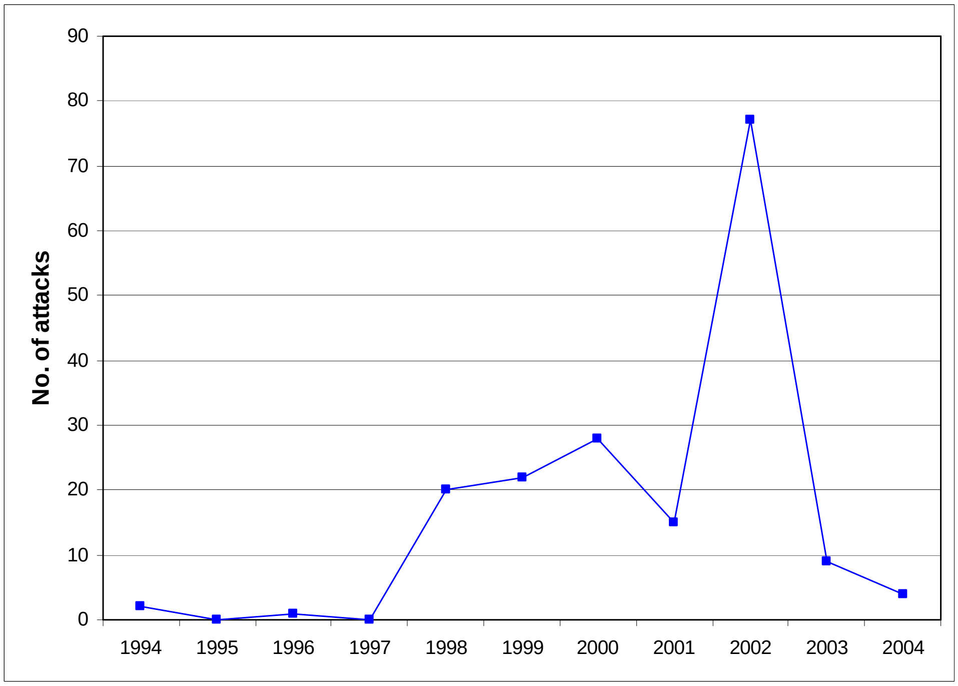
A key immediate use of the U.S./Canada DAWG database was to identify critical components that typically become disrupted. Analyzing the U.S. and Canada database revealed that the most common component disrupted in an electric power outage is the transmission system. About 90% of the outages involved a disruption of the transmission system. This finding was then compared against characteristics of terrorist attacks against electricity in other countries.

Although no direct terrorist attacks on the electric sector are known to have occurred in the United States, a number of attacks have been documented around the world over the last few decades. An initial data set for the international events was obtained from the Terrorism Knowledge Base, a database maintained by the National Memorial Institute for the Prevention of Terrorism [4].

Figure 6 shows the number of international terrorist attacks specifically on the electricity sector for the period 1994-2004. The countries included in the database for this period are Colombia, Spain, France, Russia, Albania, Turkey, Brazil, Chile, Georgia, Indonesia, Iraq, Israel, Kashmir, Kosovo, Latvia, Nepal, Pakistan, Paraguay, Peru, Sri Lanka, Sudan, Sweden and Tajikistan. Of the total number of attacks, our analysis of the data shows that 65.2% took place in Colombia and 6.7% in Spain. The rest of the countries accounted for less than 5% each. The origin of the sudden rise in attacks in 2002 is not currently known, but is probably a function of a change in terrorist tactics within Colombia, which accounted for 87% of the attacks in that year.

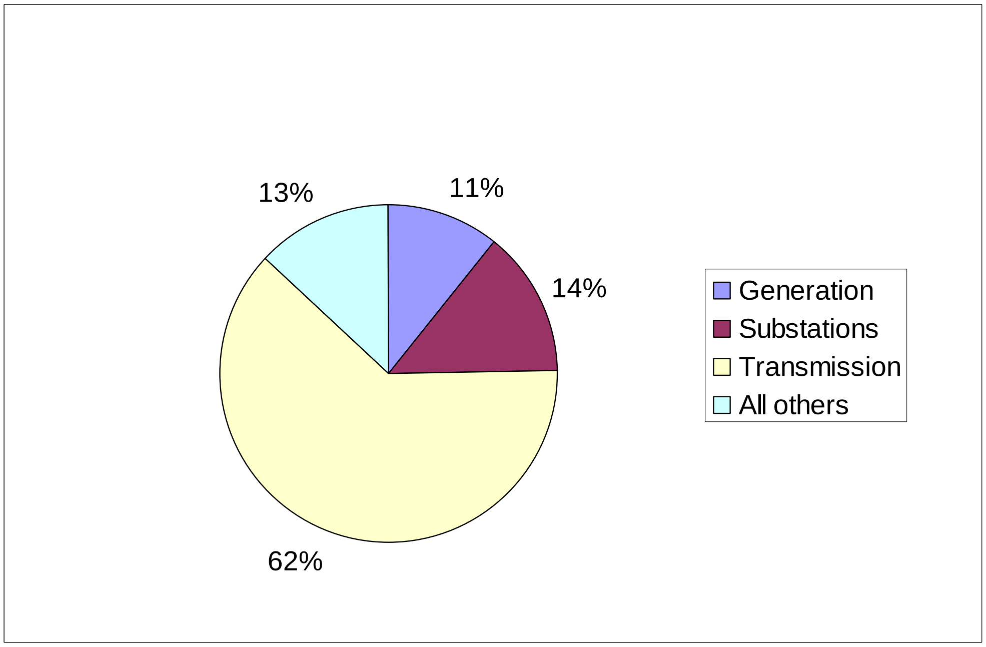
Information about the kinds of components attacked is also available for these incidents. As Figure 7 shows, transmission lines are the most common targets. Over 60% of the attacks recorded for this period were to transmission systems. The data were categorized as follows. *Generation* includes power stations and dams. The category *substations* includes substations and transformers. *Transmission* includes power grids, pylon and utility towers. *All others* includes distribution, electric relays, human resources, junction boxes, offices, storage, vehicles, etc. In terms of number of attacks, this information suggests that transmission lines are the most vulnerable component of the electricity infrastructure.

Figure 6. Number of International Terrorist Attacks on Electricity Infrastructure: 1994-2004



Source: Graphed from a database extracted from the National Memorial Institute for the Prevention of Terrorism (MIPT) data.

Figure 7. Components of Electricity Infrastructure Attacked in International Events (Total Number of Events = 183)



Source: Compiled from a database extracted from the National Memorial Institute for the Prevention of Terrorism (MIPT) data.

Thus, both data sets indicate that transmission systems are a key vulnerability, yet as the database of terrorist attacks shows, other components such as substations also present threats. This provides the basis for the construction of various scenarios to portray alternative ways in which electric power systems could become disrupted and the ultimate consequences of such patterns of disruption. The scenarios at the level of the bulk electric power system combine alternative configurations and disruption patterns for transmission lines, substations, and generation facilities. An extreme scenario would be an area served by few transmission lines coming in at locations that require the lines to enter via very few corridors and be close together, combined with very few substations and no in-region generation capacity. Each scenario when combined with the specific characteristics of an urban area or region generates other scenarios that link to urban area population and business size and characteristics.

Understanding the Consequences of Attacks against the Electricity Sector

Efforts to identify the potential effect of failures in the electricity sector on other infrastructure systems have been made using the concept of interdependencies among different infrastructures and between infrastructure and other sectors of the economy. Interdependencies have been underscored in the engineering literature, along with the potential for cascading effects to occur when one system affects another [5]. In economics, input-output techniques have been applied to the identification of infrastructure interdependencies [3]. Although much of the literature has focused on the conceptual basis for such interdependencies, efforts at quantifying interdependencies based on individual incident data are beginning to emerge.

For example, interdependencies have been quantified by Zimmerman [7] as an “effect” ratio that compares the number of times infrastructure systems impact one another. Using an illustrative database of about 100 cases, the ratio of the number of times a particular type of indicator affected others vs. the number of times others affected it were as follows for different kinds of infrastructure - water mains: 3.4; roads: 1.4, gas lines: 0.5; electric lines: 0.9; fiber optic/telephone: 0.5; and sewers and sewage treatment: 1.3.

Zimmerman and Restrepo [8] developed another simple measure of interdependency in the context of electric power outages and their effects on other sectors. That work analyzed electric power outage characteristics from secondary data for the August 14, 2003 outage in the U.S. and Canada as well as using data constructed for selected cases from 1990-2004 outages in the U.S. and Canada. The indicator compared the duration of outages in the initial electric power outage with the duration of the outages of specific public services and businesses affected, defined as the time to recover services.

For the August 14, 2003 electricity outage, results from the Zimmerman and Restrepo paper [8] showed that the duration of outages linked to the electricity outage for affected public services exceeded the duration of the initial power outage itself. In other words, they were cascading events that escalated. Rinaldi, Peerenboom and Kelly [5] define cascading infrastructure events as those that affect other infrastructure systems, and escalating events as a type of cascading event where the magnitude of the effect on the secondary infrastructure affected is greater than that of the initial infrastructure. However, for industrial establishments, the results were less clear with impacts ranging from being far less than the duration of the initial power outage to far more, generally depending on the amount of damage to equipment. For example, extensive damage can occur when substances in industrial furnaces are not removed fast enough, resulting in cooling and hardening, making it difficult to remove the material. In this case, a relatively short-lived power outage can result in a longer-duration idling of industrial production.

Results from the larger events database were less clear. A number of outages showed durations in infrastructures affected as being less than the duration of the overall outage, primarily because of the use of backup power.

Economic Assessments

The identification of consequences provides a basis for conducting economic assessments. A couple of frameworks are used for this purpose. One uses service delay factors. Another uses value of life and injury estimates for more severe impacts. Results for public services and businesses tend to differ, and applications of economic assessments to each of these areas are briefly summarized below.

Public Services

For public services, economic assessments are being determined in a few ways. First, standard cost of delay estimates for users were assembled and applied to an affected base usually in terms of total population. For example, in the area of transportation, delays per person hour are typically valued at a relatively set amount for workers. For automobile travel, each hour of delay, for example, has been valued at between 50% and 100% of the hourly wage [2]. These can be applied to the amount of time and number of people delayed stratified by a wage distribution for that population. For transportation, costs may be associated with a variety of factors such as the cost of switching to another mode of travel; for water supply, costs may be the cost of switching to another source of water. Second, extreme event databases were tapped for public services and other kinds of impacts to obtain value of life and injury estimates as well as business losses to apply also to an affected base.

Businesses

For businesses, few multipliers exist, other than those generated at a relatively macro scale from input-output techniques. Total costs and costs per unit time of a business outage for specific events, such as blackouts, extreme weather conditions, and earthquakes are usually obtained from surveys. Cost factors applied to public services are often directly applied to businesses as well, but insurance estimates are more typically a basis for assessing the economic impacts of business losses. This work is still in progress.

CONCLUSIONS

Using event databases for both non-terrorist and terrorist causes coupled with consequence and economic assessment provides the basis for a framework for decision-makers in several ways. First, it enables a refinement in the analysis of consequences by providing statistically based vulnerability analysis that can estimate customers affected or duration of outages from other characteristics of the outages. Second, it provides a means to identify components of the electric power system typically disrupted rather than hypothetically identifying such components. These can then be linked to affected users or user groups to allow for economic assessment. Third, it enables indicators of infrastructure interdependencies to be constructed as a means of identifying the general direction of impacts from such interdependencies.

REFERENCES

[1] J. Apt, “Grid Realities: Blackouts are Inevitable Survival of Critical Missions,” Presentation at the ANSI Summit on Enterprise Power Security & Continuity, March 16, 2005.

[2] ECCONORTHwest and PBQD, “Estimating the Benefits and Costs of Public Transit Projects. TCRP Report 78, 2002. Available at: http://gulliver.trb.org/publications/tcrp78/index.htm.

[3] Y. Haimes and P. Jiang, “Leontief-model of risk in complex interconnected infrastructures,” *Journal of Infrastructure Systems* 7 (1), pp. 1-12, 2001.

[4] National Memorial Institute for the Prevention of Terrorism. Terrorism Knowledge Base. Available at: http://www.mipt.org

[5] S.M. Rinaldi, J.P. Peerenboom, and T.K. Kelly, “Identifying, Understanding and Analyzing Critical Infrastructure Interdependencies,” *IEEE Control Systems magazine*, pp. 11-25, December, 2001.

[6] U.S. Census Bureau. Mini-Historical Statistics. No. HS-1. Population: 1900 to 2002. Available at: http://www.census.gov/statab/hist/HS-01.pdf.

[7] R. Zimmerman, “Decision-making and the Vulnerability of Critical Infrastructure,” *Proceedings of IEEE International Conference on Systems, Man and Cybernetics*, edited by W. Thissen, P. Wieringa, M. Pantic, and M. Ludema. The Hague, The Netherlands: Delft University of Technology, 2004. ISBN: 0-7803-8567-5.

[8] R. Zimmerman and C. Restrepo, “The Next Step: Quantifying Infrastructure Interdependencies to Improve Security,” *International Journal of Critical Infrastructures*, forthcoming, Fall 2005. UK: Inderscience Enterprises, Ltd.