Information Technology (IT) and Critical Infrastructure Interdependencies for Emergency Response

Rae Zimmerman
Professor of Urban Planning
Robert F. Wagner Graduate School of Public Service
New York University
rae.zimmerman@nyu.edu

Carlos E. Restrepo
Associate Research Scientist
Robert F. Wagner Graduate School of Public Service
New York University
cer202@nyu.edu

ABSTRACT

Information technologies and other critical infrastructures are interconnected in ways that can lead to vulnerabilities in the ability of these infrastructures to perform during natural disasters and acts of terrorism either to reduce adverse consequences or provide needed emergency response services. This research applies and adapts a number of indicators of infrastructure interdependency based on the authors' earlier research to determine where weak points and strengths occur in the interconnections between infrastructure technology and other infrastructure support services such as electric power and transportation, and where weak points create vulnerability that can be improved for more effective response in emergencies.

Keywords

Critical Infrastructure; Interdependencies; Emergency Response

INTRODUCTION

Information technologies play an undeniably central role in sustaining emergency response capacity in almost any catastrophe. One of the ways in which this critical support is sustained is through the viability of the various interconnections between information technology and other critical infrastructures. The general areas of infrastructure interdependence have been recognized for some time (Rinaldi et al., 2001; Zimmerman, 2006), and refer to both functional and spatial relationships (Zimmerman, 2005). According to Rinaldi et al. (2001), interdependence can result in escalating failures, that is, interdependence increases the magnitude of damage over what might have happened from the failure of a single infrastructure. Critical infrastructures include electric power, transportation, telecommunication, water, and environmental protection infrastructure (National Research Council, 2002), and the criticality of these infrastructures has been emphasized in numerous federal government homeland security documents. On the one hand, information technologies support these other infrastructures, for example, by providing computerized detection and control systems (Zimmerman and Horan, 2004a). On the other hand, these other infrastructures support information technologies, for example, such information technologies are dependent upon electric power in order to function or at least to function over a long period of time. These interdependencies require quantification to capture the relationships more precisely (Zimmerman and Restrepo, 2006). The development and application of technologies for information, other critical infrastructure, and emergency response services are generally proceeding independently of one another so that interdependencies are often not an explicit part of the design. This issue needs to be confronted to avoid magnifying effects during emergencies and to enable both information technology and other critical infrastructures to support emergency response more effectively.

APPROACH

This research has adopted the following approach to identifying and characterizing the role of information technologies and critical infrastructure in security and protection from adverse consequences of natural hazards and terrorist actions. The research is based on databases of events obtained from documents and news media accounts of accidents in which two or more infrastructures were involved, one of which was an information infrastructure technology. First, literature reviews and case analyses are used to identify vital connections that occur between information technologies and infrastructure for the events to locate key functional interdependencies as well as co-

location. These are used as a basis of characterizing or codifying types of accidents. Second, weaknesses and vulnerabilities in these connection points, as well as opportunities to achieve risk reduction and risk management by means of these connections, are examined by means of case analyses representing success stories as well as accident events. Third, interdependency indicators developed by earlier research by the authors are applied to infrastructures that depend on information technology as well as to the linkage between information technology and those infrastructures as a means of quantifying these relationships. Finally, the implications of interdependencies between information technology and critical infrastructures for the effectiveness of emergency response are evaluated.

PRELIMINARY RESULTS

Evidence of Information Technology and Critical Infrastructure Interdependencies

Society's dependence on infrastructure is escalating and the dependence of infrastructure on information technology is substantial and increasing. In practically all infrastructure sectors – electric power, transportation, water, and telecommunications – capacity and usage is growing at rates that often exceed the rate of population growth (Zimmerman and Horan, 2004b). The interdependencies between information technologies and the viability of these critical infrastructures are large and are also increasing, though these trends are not as easy to quantify. Henry and Dumagan (2004: 155), for example, identify the extent of the dependency in an aggregate way: "Between 1996 and 2001, infrastructure industries, which together accounted for 8-9 percent of the nation's Gross Domestic Product (GDP), owned about one-third of all capital stock in information technology (IT) equipment and software."

Evidence of Vulnerabilities Created by Interdependency

Some examples of the vulnerability of this interdependency from our research are noteworthy, in particular, in the interdependencies between information technology and the electric power sector. The August 2003 blackout in North America underscored the delicate and critical role information technologies can play in supporting other infrastructure. In that massive outage, three failures of information technology systems – alarm systems, software, and other computerized controls – were associated at least in part with the outage (U.S.-Canada Power System Outage Task Force, 2004). In 1999, the Olympic Pipeline in Washington experienced a major failure due to the failure of its computer control system, which ultimately led to an inability to control pressure resulting in three deaths. In 2004 a Sasser worm was able to disrupt an oil and gas platform in the Gulf of Mexico for a couple of days. Hacking and other cyber attacks have disrupted energy and other infrastructure facilities. Information technology has numerous interconnections in the water supply and wastewater treatment sector, and vulnerabilities have surfaced in areas such as the inability to track contaminants or properly characterize flow rates (Zimmerman, 2004b). Interdependency between information technologies and transportation infrastructure is also noteworthy. Quite a number of examples exist where airline travel was halted due to computer failures in air controller operations or within other airport operations, such as ticketing or automated baggage handling systems.

Indicators of Infrastructure Interdependency

Indicators of Relative Effect of Infrastructures on One Another. Infrastructure interdependence and interconnectivity and its effect on infrastructure performance have received considerable attention, and efforts to quantify these characteristics are emerging. One indicator developed by Zimmerman (2004a) used the extent to which a failure in one type of infrastructure was more likely to affect other infrastructure as opposed to that infrastructure being affected by failures in other infrastructure systems. The indicator was applied to distribution systems in electric power, transportation, water, and telecommunications. Using an illustrative database, the frequency of telecommunication infrastructure being affected by other infrastructure failures (e.g., water main breaks or electric power outages) was greater than the frequency that telecommunications outages affected other infrastructure. It should be kept in mind that the database used to construct these indicators was illustrative (based on about 100 cases), and another database might have revealed different relationships.

Indicators of Outage Duration. A second indicator (Zimmerman and Restrepo, 2006) provided a comparison between the duration of an electric power outage with the duration of another infrastructure affected by the power outage. A ratio greater than one implies that the infrastructure dependent on electric power takes longer to recover than the electric power system does. This simple indicator was applied to the recovery of oil and gas facilities after Hurricanes Katrina and Rita. Results of the authors' research showed that refineries were more likely to be out longer than electric power. The ratios for six refineries in Louisiana ranged from slightly over 1.0 to just over 3.0, and were never less than 1.0, indicating that refineries needed more time even after the power was up to readjust and

become operational. In contrast, pipeline outages were more likely to equal the duration of the electric power outages. Refinery and pipeline outages were due to a number of factors, such as some voluntary shutdowns to avoid damage, damage to those that were not shut down, electric power outages, telecommunication outages from electric power outages or direct damage.

Indicators of Spatial Concentration of Information Technology and Other Infrastructure. A third indicator to characterize information technology, its relationship to other infrastructures, and its potential vulnerability is the degree to which facilities, their capacity, value and/or usage are concentrated geographically. This issue is only beginning to be recognized (Parfomak, 2005). Concentration is measured in a number of different ways. One way is directly in terms of the distribution of these infrastructure characteristics (number of facilities, capacity, value or usage) at some geographic level, e.g., the state, municipality, or within municipalities. A second measurement is using location quotients, which is a standard measure of industrial activity in regional economics (see for example, Bendavid-Val, 1991: 130-133). Location quotients, like direct measures of infrastructure characteristics also can be applied to any geographic area. Some preliminary findings with respect to the direct measures show definite concentrations of practically all different kinds of infrastructure throughout the U.S. For example, although the internet is considered to be a highly dispersed and distributed system, concentrations occur at a number of points, for example, the limited number of domain name servers and the limited number of corridors over which major fiber optic cable travels. In the area of telecommunication, about half of high speed lines, total loops are in the top 8 states and about half of all mobile wireless subscribers are located in the top 8 states, indicating a high degree of concentration of both facilities and usage. Similarly, our research has shown that energy and transportation infrastructure capacity and usage are highly concentrated with about half of the infrastructure (no matter how it is measured) usually being located in well-under a dozen states. This implies that at least at very broad geographic levels there is spatial interdependence among a wide variety of different kinds of infrastructure.

Interdependencies and Emergency Response

Emergency response is heavily dependent upon traditional infrastructures, in particular, transportation capacity, electric power and telecommunications. Transportation capacity in major cities in the United States has shown a declining trend at critical times during the day as indicated by congestion. Congestion measured as hours of delay continues to rise, producing a potential threat to needed emergency response resources. Telecommunication failures in emergencies are now well-known, and though new technologies are emerging rapidly, access to them is relatively limited.

CONCLUSIONS

Interdependencies between information technology and critical infrastructures are pervasive. While information technology is a potential enhancement for infrastructure, the rate at which it has developed has not always enabled the infrastructure that it supports to keep pace, thus presenting potential vulnerabilities. This can escalate impediments that already exist between conventional infrastructure and emergency response capabilities. The development and application of technologies for information, other critical infrastructure, and emergency response services are generally proceeding independently of one another so that interdependencies are often not an explicit part of the design. This issue needs to be confronted to avoid magnifying effects during emergencies and to enable both information technology and other critical infrastructures to support emergency response more effectively. The development and application of quantified indicators are critical to understanding interdependency phenomena. Examples of such indicators from the authors' research are those that portray (1) which infrastructures more commonly affect others, (2) what the relative delay in recovery times is for one infrastructure, such as electric power, relative to another that it disables, and (3) the spatial concentration of infrastructures relative to one another.

ACKOWLEDGEMENTS

This work is supported by a number of research grants from the U.S. Department of Homeland Security under Grant Numbers N00014-05-1-0630 of the Office of Naval Research through the Center for Risk and Economic Analysis of Terrorism Events (CREATE) at the University of Southern California; 2003-TK-TX-0003, the Institute for Information Infrastructure Protection (I3P) Dartmouth College; and M9002-F5611 and M9003-F5611 through the Center for Catastrophe Preparedness and Response (CCPR) at NYU. Points of view in this paper are those of the author(s) and do not necessarily represent the views of the U.S. Department of Homeland Security.

REFERENCES

1. Bendavid-Val, A. (1991) *Regional and Local Economic Analysis for Practitioners*. 4th edition. Westport, CT: Praeger.
2. Henry, D. and Dumagen, J. (2004) Economics, in R. Zimmerman and T.A. Horan, eds., *Digital Infrastructures: Enabling Civil and Environmental Systems through Information Technology*, London, UK: Routledge.
3. National Research Council (NRC) (2002) *Making the Nation Safer: The Role of Science and Technology in Countering Terrorism*, Washington, D.C.: National Academy Press.
4. Parfomak, P.W. (2005) *Vulnerability of Concentrated Critical Infrastructure: Background and Policy Options*, Washington, DC: Congressional Research Service, December 21.
5. Rinaldi, S.M., Peerenboom, J.P. and Kelly, T.K. (2001) Identifying, Understanding and Analyzing Critical Infrastructure Interdependencies, *IEEE Control Systems magazine*, pp. 11-25. December.
6. U.S.-Canada Power System Outage Task Force (2004) *Final Report on the August 14th 2003 Blackout in the United States and Canada: Causes and Recommendations*. The Task Force, April.
7. Zimmerman, R. (2006) Critical Infrastructure and Interdependency, in *The McGraw-Hill Homeland Security Handbook*, David G. Kamien, ed. NY, NY: The McGraw-Hill Companies, Inc., pp. 523-545.
8. Zimmerman, R. (2004a) 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.
9. Zimmerman, R. (2005) Social Implications of Infrastructure Network Interactions, Chapter 4 in O.Coutard, R. E. Hanley and R. Zimmerman, eds. *Sustaining Urban Networks*. London, UK: Routledge, pp. 67-85.
10. Zimmerman, R. (2004b) Water, Chapter 5 in R. Zimmerman and T. Horan, eds. *Digital Infrastructures: Enabling Civil and Environmental Systems through Information Technology*. London, UK: Routledge, pp. 75-95.
11. Zimmerman, R. and Horan, T. eds. (2004a) *Digital Infrastructures: Enabling Civil and Environmental Systems through Information Technology*. London, UK: Routledge.
12. Zimmerman, R. and Horan, T. (2004b) What are Digital Infrastructures? Chapter 1 in R. Zimmerman, and T. Horan, eds. D*igital Infrastructures: Enabling Civil and Environmental Systems through Information Technology*. London, UK: Routledge, pp. 3-18.
13. Zimmerman, R. and Restrepo, C. E. (2006) The Next Step: Quantifying Infrastructure Interdependencies to Improve Security, *International Journal of Critical Infrastructures*, 2006. UK: Inderscience Enterprises, Ltd. www.inderscience.com.