RESEARCH BRIEF

Institute for Homeland Security Solutions
Applied research • Focused results

March 2010

Methods for Assessing Vulnerability of Critical Infrastructure

Project Leads

Eric Solano, PhD, PE, RTI International

Statement of Problem

Several events in the recent past, including the attacks of 9/11 and Hurricane Katrina, revealed the lack of plans to protect infrastructure from destructive threats and prompted the need to work on preparedness, response, and recovery plans related to infrastructure safety.

To work on preparedness, response, and recovery plans, given the scarce resources available, it is necessary to select infrastructures for protection and decide how they will be protected against potential threats. To accomplish these goals, policymakers will benefit from data and information derived from risk, vulnerability, and resilience assessments and scenario simulations. Vulnerability and resilience are related to risk in that reducing vulnerability will reduce risk and increasing resilience may reduce the consequences of a disaster.

The research question that motivates this brief is whether an inclusive approach that incorporates physical, social, organizational, economic, and environmental variables in addition to empirical measurements and operationalization of resilience and vulnerability will help to improve the understanding and management of risk associated with threats to complex infrastructure systems.

This brief reviews recent literature in vulnerability and resilience assessment, summarizes the most important findings, and suggests future directions to advance the field of vulnerability and resilience research.

Background

An objective of the Department of Homeland Security's Human Factors and Behavioral Sciences Division is to "Enhance preparedness and mitigate impacts of catastrophic events by delivering capabilities that incorporate social, psychological and economic aspects of societal resilience." Infrastructure vulnerability and resilience are intricately related with community resilience. Research conducted to enhance methodologies and practical measurements of vulnerability and resilience must try to include (in addition to the physical dimension) the social, organizational, economic, and natural environment dimensions.

Cutter et al. (2008) mention important gaps in the research field of vulnerability. There is still progress to make in the identification of standards and metrics for measuring disaster resilience; in the advancement of a theoretical framework and practical applications of vulnerability; in the articulation of the relationship between vulnerability, resilience, and adaptive capacity; and in the explanation of the causal structure of vulnerability. It is not obvious what leads to resilience within coupled human-physical-environment systems or what variables should be utilized to measure it.

There have been few attempts to combine all factors that contribute to vulnerability. Conceptual models for hazard vulnerability fail to address the coupled human-environment system associated with the proximity to a hazard, and they fail to include a temporal dimension that shows where vulnerability begins and ends.

Advancing the field of vulnerability and resilience assessment will also have important policy implications. Arboleda, Abraham, Richard, and Lubitz (2009) indicate that after the disaster event, infrastructure managers must prioritize the allocation of restoration resources to meet the demand at critical facilities. Baker (2008) helps develop an investment strategy to improve system resilience. His method provides a snapshot of system conditions as a baseline for future improvements. Egan (2007) highlights that large technical systems create challenges for policymakers in the form of negative externalities, the risks of failure and disasters, and problems with management, control, and coordination. He argues that an effective policy would be to establish liability rules based on the notion that organizations should internalize the costs of the risks they produce and that by internalizing them, they will make wiser choices about the technologies they use.

This brief summarizes the most important findings about vulnerability and resilience assessment from a few reviewed papers.

The methodologies reviewed, in general, fail to incorporate the social and organizational components into the analysis of physical infrastructures. This is arguably the most important deficiency found in the current methodological and empirical practices to measure vulnerability and resilience. The interdependencies among physical and human components in infrastructure seem to be very strong and complex. Bea (2009) argues that no matter how much physical science and technology are involved in a complex system; no system is ever solely physical or technical. Their investigative report of a failed offshore oil and gas drilling and production platform in the North Sea noted that the majority of the causes of this failure (80% or more) were firmly rooted in human, organizational, and institutional malfunctions. The remaining causes could reasonably be attributed to malfunctions in the engineered parts of this complex system.

Human factors, such as decision making related to infrastructures operations and maintenance, are considered in just some of the reviewed papers (Baker, 2008; Hellstrom, 2007; Egan, 2007).

From a methodological point of view, most methods propose mathematical modeling through network theory (Lewis, 2006; Arboleda et al., 2009; Ouyang, Hong, Maoa, Yuia, and Qi, 2009; Eusgeld, Kroger, Sansavini, Schläpfer, & Zio 2009). Graphs are implemented to represent the infrastructures' topology and their interdependencies. In addition to network theory, Lewis (2006) uses principles of logic, probability, and cost minimization.

Others propose the elicitation of expert judgment (Parks & Rogers, 2009; Ezell, 2007; Egan, 2007; Cooke & Goossens, 2004) and qualitative assessments (Baker, 2008; EPA, 2002; Haimes & Longstaff, 2002). Table 1 summarizes some important features of these selected publications and shows the heterogeneity across these methodologies.

Most methods use linear optimization to solve for minimum-cost scenarios and do not include more extensive nonlinear capabilities. Some authors mention analysis of uncertain values for model parameters (Ezell, 2007; Cooke & Goossens, 2004; Lewis, 2006). The importance of assessing and protecting cyberspace is a key aspect in some methods (Baker, 2008; Parks & Rogers, 2009; Hellstrom, 2007; Haimes & Longstaff, 2002; Egan, 2007). Some authors discuss the use of Supervisory Control and Data Acquisition (SCADA) as a control system for critical infrastructures (Baker, 2008; EPA, 2002; Haimes & Longstaff, 2002; Lewis, 2006).

The reviewed methodologies are further analyzed and compared using a number of characteristics. Table 2 shows a matrix with values assigned for each characteristic across all reviewed methods. This brief uses a qualitative method to evaluate each characteristic by the level of detail (high, medium, or low) in which it was described.

Table 1. Evaluated Properties Across Reviewed Publications

Reference	1	2	3	4	5	6	7	8	9	10	11	12
Mathematical modeling			x	x		x				x	x	x
Linear programming			x	x						x		x
Network theory			x	x						x		x
Nonlinearity			x	x						x		x
Human factors	x						x		x			
Cyberspace	x				x		x	x	x			
Static			x	x								x
Dynamic			x							x		x
Uncertainty						x					x	x
Spatial distribution	x											
Expert judgment			x		x	x			x		x	
Interdependencies	x		x	x			x	x	x	x		x
Environment									x			
Agent-based			x									
Simulation			x	x		x				x		
Qualitative	x	x				x		x			x	
Quantitative			x	x		x					x	x
Definition: vulnerability	x	x				x	x					x
Definition: criticality	x	x				x	x	x	x	x		x
Definition: risk	x					x	x					x
Definition: complexity							x	x	x	x		
SCADA	x	x						x				x

Table 2. Evaluated Dimensions Across Reviewed Publications

Reference	1	2	3	4	5	6	7	8	9	10	11	12
Scope	L	M	H	H	M	M	L	M	M	H	M	H
System characterization	M	H	H	H		H			M			H
Process definition	H	L	H	H	M	H	H	M	H	H	M	H
Commonality	M	L	L		L				L			M
Extensibility	L		M	L	L	L			L	L	L	
Scalability	M		L							M		L
Comprehensiveness	L	L	L				M					
Strategic and policy implications	M	M	H	M	L	L	M	M	H			H
Results	M	M	H	L	L	M	M	L	H	M		

Level of detail: H = high, M = medium, L = low.

An important aspect of these methodologies is system definition and characterization. Lewis (2006) provides a high level of detail to characterize the systems through networks. Networks can be scale-free networks (nonrandom networks around critical nodes) or small-world networks (around clusters of noncritical nodes). Arboleda et al. (2009) define a graph with demand, trans-shipment, and supply nodes; because some of the nodes are part of two or more infrastructure networks, the connections between the different infrastructure systems create interdependencies. Ouyang et al. (2009) define a graph for the electrical network and for a gas pipeline system.

Another important characteristic of these methods is process definition. Lewis (2006) defines the Model-Based Vulnerability Analysis (MBVA) based on principles of logic, probability, and cost minimization. The MBVA process includes a list of assets, a network analysis, a model using fault-tree method, and analysis of the fault tree using an event tree. Given threat probabilities, the objective of this method is to enumerate all possible event combinations and to compute the probability for the infrastructure to fail under each event scenario. Arboleda et al. (2009) include the analysis of external infrastructure systems through optimization techniques (facility operations, post-disaster condition, and restoration) and analysis of internal capabilities through systems dynamics (flow of people). Once the system has been defined in a graph, Ouyang et al. (2009) run optimization models for assessing the functional vulnerability of the electric power and gas pipeline systems.

Another important characteristic analyzed was the set of results generated by these methods. Baker (2008) provides a summary of the assessment results for each mission-critical system in the facility. Arboleda et al. (2009) provide results from the proposed models. The basic model results are the flows of commodities that minimize the cost of the operation. The results of a second model consist of a quantification of the supply reduction due to a disaster event. The third model results are the restoration strategies that minimize a weighted sum of the operational cost of the infrastructure systems.

Additional characteristics analyzed for these methods include commonality, extensibility, scalability, and comprehensiveness. Examples for each of these characteristics follow.

The U.S. Environmental Protection Agency (2002) indicates in its vulnerability assessment factsheet that single points of failure could be common to many facilities. Ouyang et al. (2009) indicate that their method can be extended by adding more complex interdependencies between two infrastructures. Eusgeld et al. (2009) indicate that for the model scenarios to be scaled up, the main issues to overcome are the slow simulation speed and the large number of parameters to be input into the model. Baker (2008) argues that his method is comprehensive, since assessed threats could be both cyber and physical attacks/sabotage and hazards can be natural disasters or normal accidents.

Tables 1 and 2 show a range of characteristics and dimensions evaluated across a number of proposed methods to assess vulnerability of critical infrastructures. It is evident from these preliminary evaluations that most methods, if not all of them, are still in their early development stages and still lack important properties toward qualifying as more robust tools with realistic representations of complex systems.

Synthesis

A dozen methodologies to assess vulnerabilities of critical infrastructures were reviewed and evaluated across a number of characteristics. Tables 1 and 2 show that although some of these methodologies show a considerable amount of development for one or two characteristics, they lack the necessary detail in other areas to make them more realistic methods, specifically because they fail to incorporate additional analytical dimensions (i.e., social, organizational, environmental, and economic dimensions).

The modeling technologies are also limited to the capabilities of network theory to represent infrastructure topologies. Many of these methods are not appropriate to answer the following research question:

> Can a holistic, multi-disciplinary, multi-dimensional framework, in addition to methodological and empirical improvements to measure vulnerability and resilience, help to better understand and manage the risks of infrastructures under threats?

Future Directions

Future work in this area must be motivated by the intellectual quest highlighted above. The inclusion of social, organizational, and environmental variables in addition to the engineering definitions for resilience and vulnerability will help generate more realistic representations of complex infrastructure systems.

Mathematical modeling will remain a very important tool for future development in this area although it is important to explore different technologies in conjunction to graph/network theory to overcome many of the limitations related to network topologies. The use of geographic information systems (GIS) could also bring a lot of benefits by representing infrastructures and their interrelationships through more realistic geographic topologies.

In addition to better topological representations, future work should also explore using more simulation technologies to incorporate uncertainty analyses. Simulations of human interactions with infrastructures also need to be enhanced. The addition of these technologies will bring more accurate representations of the reality, but will also increase the computational requirements. High performance computing solutions are recommended to be able to more efficiently scale up the representations of problems related to critical infrastructures.

Contact Information

Eric Solano
RTI International
3040 Cornwallis Road
Research Triangle Park, NC 27709
919-485-2655
solano@rti.org

Eric Solano, PhD, PE, is a research engineer/analyst with RTI, where he applies his training as a civil and environmental engineer and his experience with multiple information technology tools to design and develop engineering solutions and to develop computer-based tools for a variety of engineering projects. His primary area of expertise is systems analysis and modeling for environmental and civil engineering. More recently, he has been involved with the use of high-performance computing tools in simulations, modeling, and programming. He develops and analyzes engineering systems that require modeling and uses technologies such as linear programming optimization and decision-support systems. Other technologies included in his interests are genetic algorithms, neural networks, nonlinear optimization, and stochastic optimization. Dr. Solano has a PhD in civil engineering from North Carolina State University and is a registered professional engineer in the state of North Carolina.

References

Arboleda, C. A., Abraham, D. M., Richard, J. P., & Lubitz, R. (2009). Vulnerability assessment of health care facilities during disaster events. *Journal of Infrastructure Systems, 15*(3), 149–161.

Baker, G. H. (2005, April). *A vulnerability assessment methodology for critical infrastructure sites.* Department of Homeland Security symposium: R&D partnerships in homeland security. Boston, Massachusetts. Retrieved from http://works.bepress.com/george_h_baker/2

Bea, R., Mitroff, I., Farber, D., Foster, H., & Roberts, K. H. (2009). A new approach to risk: The implications of E3. *Risk Management, 11*, 30–43. doi:10.1057/rm.2008.12.

Cooke, R. M., & Goossens, L. H. J. (2004). Expert judgment elicitation for risk assessments of critical infrastructures. *Journal of Risk Research, 7*(6), 643–656.

Cutter, S. L., Barnes, L., Berry, M., Burton, C., Evans, E., Tate, E., & Webb, J. (2008). A place-based model for understanding community resilience to natural disasters. *Global Environmental Change, 18*(4), 598–606.

Egan, M. J. (2007, March). Anticipating future vulnerability: Defining characteristics of increasingly critical infrastructure-like systems. *Journal of Contingencies and Crisis Management, 15*(1), 4–17. doi:10.1111/j.1468-5973.2007.00500.x

Eusgeld, I., Kroger, W., Sansavini, G., Schläpfer, M., & Zio, E. (2009). The role of network theory and object-oriented modeling within a framework for the vulnerability analysis of critical infrastructures. *Reliability Engineering & System Safety, 94*(5), 954–963.

Ezell, B. C. (2007). Infrastructure Vulnerability Assessment Model (I-VAM). *Risk Analysis, 27*(3), 571–83.

Haimes, Y. Y., & Longstaff, T. (2002). The role of risk analysis in the protection of critical infrastructures against terrorism. *Risk Analysis, 22*(3), 439–44.

Hellstrom, T. (2007). Critical infrastructure and systemic vulnerability: Towards a planning framework. *Safety Science, 45*(3), 415–430.

Lewis, T. (2006). *Critical infrastructure protection in homeland security: Defending a networked nation.* John Wiley and Sons, Inc.

Ouyang, M., Hong, L., Maoa, Z., Yua, M., & Qi, F. (2009). A methodological approach to analyze vulnerability of interdependent infrastructures. *Simulation Modelling Practice and Theory, 17*(5), 817–828.

Parks, R. C., & Rogers, E. (2008). Vulnerability assessment for critical infrastructure control systems. *IEEE Security & Privacy, 6*(6), 37–43.

United States Environmental Protection Agency. (2002, November). *Vulnerability assessment factsheet.* Office of Water (4601M); EPA 816-F-02-025. Retrieved from www.epa.gov/ogwdw/security/index.html