

Journal of Homeland Security and Emergency Management

Volume 3, Issue 4

2006

Article 4

Enhancing Homeland Security: Development of a Course on Critical Infrastructure Systems

George H. Baker III*

Richard G. Little†

*Associate Professor, Integrated Science and Technology, James Madison University, bakergh@jmu.edu

†Director, Keston Institute for Infrastructure, University of Southern California, rglittle@usc.edu

Copyright ©2006 The Berkeley Electronic Press. All rights reserved.

Enhancing Homeland Security: Development of a Course on Critical Infrastructure Systems

George H. Baker III and Richard G. Little

Abstract

The rise of the American homeland security endeavor has created demands for knowledgeable professionals to address issues of critical infrastructure assurance. James Madison University has recently developed a survey course on infrastructure performance using a complex systems approach. Course development was facilitated by the enthusiastic support and participation of a multi-disciplinary faculty team. The course is designed for a broad student audience including physical science, public administration, health, business, economics and sociology majors. The course has been successful in terms of graduate and undergraduate student enrollment and has generated positive student feedback.

Drawing on recent work from the physical, engineering, and social sciences, we take an interdisciplinary approach to understanding complex system operation and failure. We begin by considering historical examples of major system failures. We then explore the components, operation, and complex interdependencies of the infrastructures most critical to society. We divide critical infrastructures into three classes – commodity, service, and information – and focus on the electric power, health services and telecommunication sectors as representative examples.

Students are exposed to literatures that inform their understanding of large, complex, and risky technical systems. Course material illustrates how complex systems engender unexpected interactions of failures to occur that can result in a cascade of increasingly serious disturbances often culminating in disaster. A major component of the course is devoted to defining and measuring risk. The final instruction block is devoted to risk management strategies involving both technology and public policy. The course concludes with the presentation of student projects that may address a historical complex system failure case study, an assessment of an existing infrastructure system, or survey a specific topic on complex system operation and failure.

KEYWORDS: critical infrastructure, complex systems, education, course development

Introduction

Several exigencies motivated the development of a new course on critical infrastructure at James Madison University including increased national concern about the viability of critical infrastructure systems in the context of homeland security, the advent of the new area of study in complex systems,¹ and the desire for new interdisciplinary capstone courses as part of the University's Integrated Science and Technology degree program. The course was developed by an interdisciplinary faculty team within JMU's College of Integrated Science and Technology² and the Director of the National Research Council's Board on Infrastructure and the Constructed Environment³. It was an exciting and rewarding experience due to the importance of the topic, faculty team enthusiasm, strong support from University executives, and ultimately the highly positive student response.

Highly efficient, complex, and interdependent infrastructure systems including electric power, telecommunications, transportation, water utilities, food distribution, housing and shelter, public health, finance and banking are foundations of modern societies. Beginning in the mid-1990s, the United States became acutely aware of the importance of civil infrastructures and their criticality to the nation's economy and quality of life. These systems are receiving increasing attention from national, state and local government because society depends so heavily on these large, complex systems which also make them especially attractive targets for attack. Both cyber and physical disruption of these systems is possible and can result in human casualties as well as severe economic losses. These systems are also susceptible to disruption from natural disasters, which appear to be more common due to the increase in weather severity.

In the face of higher risks, understanding vulnerabilities and protecting critical systems take on a new urgency. Technological complexity, rapid social and regulatory change, and globalization contribute to making the protection of such systems very challenging. While science and technology are important parts of the solution, they are not sufficient. Effective solutions will involve an array of disciplines, including law, policy, psychology, diplomacy, security strategy, and intelligence.

¹ Watts, D. J., "Unraveling the Mysteries of the Connected Age," *The Chronicle of Higher Education*, February 14, 2003.

² Members of the original course development team included Dr. Ronald Kander, Mr. Richard Little, Dr. Ming Ivory, Dr. Michael Deaton, Dr. Maria Papadakis, Dr. Stephen Bowers, Mr. Taz Daughtrey, Mr. Ken Newbold, Dr. R.E. Burnett, Dr. Barbra Gabriel, led by Dr. George Baker.

³ R. G. Little, now Director, The Keston Institute for Infrastructure, University of Southern California.

In response to the 1995 Murrah Building bombing in Oklahoma City, the President's Commission on Critical Infrastructure Protection in the 1996-97 timeframe was a seminal effort in terms of focusing attention on infrastructure system failures and their consequences. Looking at new, post Cold War threats, the Commission's report outlined a strategy for action that stressed the importance of awareness and education and included an objective "to elevate national awareness of infrastructure threat, vulnerability, and interdependency assurance issues through education..." The report stressed the need for a "systems approach."⁴ In 2003, new homeland security strategy documents appeared that categorized critical infrastructure systems and outlined steps to protect these from physical and cyber attacks.^{5,6,7}

Explicitly addressing infrastructure education, Little has argued that present infrastructure courses, mostly associated with civil engineering departments, do not provide the interdisciplinary thinking, communication, team-building and problem-solving capabilities that lead to a needed, new class of "professional infrastructure practitioners."⁸

In the same timeframe, we were seeing an explosion in research making major inroads in understanding the behavior of complex systems. Publications by social scientists such as Duncan Watts⁹ and Charles Perrow¹⁰, and physical scientists such as Albert-László Barabási¹¹ were pioneering the exciting new science of complex systems.

Given these developments, we perceived the need for an interdisciplinary course that would introduce and survey infrastructure system architecture, operation, and failure. The course would be designed to provide a balanced treatment of technical and policy aspects of infrastructure system operation, problems, and solutions. We believed such a course would be invaluable to students interested in homeland security and public administration careers, including students majoring in science and technology as well as health services, business, and public policy (as shown in Table 1). The course would expose

⁴ Critical Foundations, the Report of the President's Commission on Critical Infrastructure Protection, Robert T. Marsh, Chairman, October 1997

⁵ National Strategy for Homeland Security

⁶ National Strategy for Physical Protection of Critical Infrastructure and Key Assets

⁷ National Strategy to Secure Cyberspace

⁸ Little, R. 1999. Educating the Infrastructure Professional: A New Curriculum for a New Discipline, *Public Works Management and Policy*. 4(2):93-99.

⁹ Six Degrees: the Science of a Connected Age, Duncan J. Watts, Norton Publishers, 2002

¹⁰ Normal Accidents: Living with High-Risk Technologies, Charles Perrow, Princeton University Press, 1999

¹¹ "Statistical Mechanics of Complex Systems," Reka Albert and Albert-László Barabási, *Reviews of Modern Physics*, Vol 74, January 2002.

students to literature providing an understanding of real infrastructure systems as complex system networks.

Course development was greatly aided by James Madison University's unique "Integrated Science and Technology" (ISAT) degree program. This program is based on the premise that the solution of technical problems involves cooperation among technical, business, policy, and social disciplines to achieve useful outcomes. The program produces technically competent graduates that also are familiar with social, economic and policy context of technical problem solving. The new infrastructure course provides a valuable "capstone" experience that integrates disciplines that ISAT students have studied separately in their first three years of the program. The course fits quite nicely into the ISAT graduate curriculum with its heavy emphasis on system analysis.

The new course was developed under the aegis of the joint James Madison University-George Mason University Critical Infrastructure Protection Program. The objective of this program is to "fully integrate the disciplines of law, policy and technology for enhancing the security of cyber networks and economic processes supporting the nation's critical infrastructures."¹²

Course Development

For the reasons just discussed, several ISAT faculty members met in the spring semester of 2003 to consider developing a course that would survey critical infrastructure systems and explore their functions, failure modes, and failure consequences. This group decided unanimously not only to proceed, but also to develop a course in time for the fall semester. Our enthusiasm led us to decide to convene the course for ourselves in the fall, whether or not a sufficient number of students enrolled.

Notwithstanding the prospect of low enrollment, we began course construction by considering the target student audience. The central question was whether to orient the course to technology majors or expand our outreach to include students in public policy, business, and other social sciences. Infrastructure assurance¹³ requires practitioners from many disciplines as diverse as civil engineering, environmental science, materials science, government operations, economics, finance, sociology, law, and political science. As a result, we believed it was appropriate to make the course available to the broader student audience. We felt the integrative nature of the course would appeal to many different majors. To spur fruitful class discussions and issue papers, we wanted

¹² CIPP Strategic Plan Objectives and Overview

¹³ Assurance connotes not just protection, but the full range of activities helpful in improving the reliability of infrastructure against threats and hazards of concern, including preparedness, prevention, protection, recovery.

students with some maturity in their chosen specialties and decided that the graduate level would be most appropriate. However, because the course would combine several specialty areas within JMU's Integrated Science and Technology major, it would be an ideal senior capstone course as well. Thus we decided to offer the course at the 400 and 500 levels, viz. ISAT 480/580, Complex Systems and How They Fail.

High on our list of objectives was the need to explain the criticality of infrastructure systems to society by surveying their components, operation, and interdependencies. On the system failure side, we felt the course should present the hazards and threats to infrastructure system operation. Then the course needed to explain how complex systems respond to these threats, often resulting in unexpected interactions of failures. Finally, we planned to address the consequences of system failures and how they may result in a cascade of increasingly serious disturbances ending in casualties and serious economic loss. To be able to quantify the relative seriousness of system failures, it was clear that the topics of risk quantification and risk management should be treated in some depth.

We wanted our students to leave the course with an in depth appreciation of our essential dependence on infrastructure systems for life, governance, social, and material well-being. We looked very closely at the bellwether findings of the President's Commission on Critical Infrastructure Protection (PCCIP) for guidance, noting their recommendation to ingrain infrastructure protection into the American culture beginning with "a comprehensive program of education and awareness."¹⁴ Although the PCCIP report stressed the cyber aspects of infrastructure assurance, we took a more balanced approach, given that the most devastating attack to our infrastructure, 9/11, had been physical.

Based on these needs and exigencies, we developed an initial list of course objectives and sketched out an initial syllabus. We felt that incorporating case studies of major system failures would expedite an understanding of the degree of societal dependence on infrastructure systems and their inherent fragility. We used several illustrative examples of disasters that "could never happen," ranging from the failure of the Maginot Line to the fall of Fortress Singapore and the sinking of the Titanic.

Initially some team members took exception to describing critical infrastructure systems as "fragile." After all, weren't these systems designed to be robust and receive constant attention to their condition? However, as we delved into the record of past system failures, everyone was surprised at the ease with which large systems can be disrupted - the Challenger space shuttle by an O-ring, or the Concorde by a small piece of runway debris. It was fortuitous that the

¹⁴ Critical Foundations: Protecting America's Infrastructures, The Report of the President's Commission on Critical Infrastructure Protection, 1997, p71.

Northeast power blackout occurred during the period of course development. This infrastructure failure served to reinforce the importance of our endeavor.

Based on our strawman syllabus, we divided the topics among team members by specialty area and began to flesh out the material. Our team members had expertise in energy systems, information technology, telecommunications, structural engineering, organizational behavior, system modeling, terrorism, hazardous materials, nuclear effects, and system vulnerability/risk assessment. We developed a schedule over the summer months to review progress and receive briefings on each topic from the responsible team member. We also solicited ideas for case studies and possible guest lecturers.

Our first progress review meeting proved cathartic. As often occurs with new projects, we realized that we had been too ambitious in the breadth of our coverage and sought ways to downsize the subject matter. One remedy was to focus on three infrastructures representing three infrastructure classes: electric power as an example of a commodity infrastructure; telecommunications as an example of information infrastructure; and the health system as an example of a service infrastructure. This approach reduced the number of illustrative case studies. We also revised the course structure, combining the stakeholder and policy units with the risk management unit, allotting two weeks for the combined topics.

We edited the learning objectives into a more succinct set as follows:

1. Develop simple, qualitative ways of thinking about complex systems, coupled with critical thinking skills concerning their operation and failure modes.
2. Understand the function of complex systems and their role in society.
3. Realize the fragility of these systems.
4. Understand why the parts making up complex systems don't sum up in simple fashion and how the individual behaviors of system parts aggregate to collective behavior.
5. Understand how vested interests affect system concepts, descriptions, and priorities.
6. Explain strategies to improve complex infrastructure resiliency.

At this meeting we reconsidered the sequence of material. We decided that the student should be exposed to some historical examples of system failures and their consequences early in the course to quickly develop a subject-matter mindset. Complex system theory would then be introduced including network science concepts and an introduction to risk. We would then use examples from infrastructure system design and operation to illustrate theoretical concepts. Instruction on real-world applications to infrastructure system would follow,

including threats/hazards, system modeling, system risk assessment, and risk management.

We decided to conclude the course with presentations of case studies on the operation and vulnerabilities of critical infrastructure systems representing our three selected sectors. In lieu of a final exam, students would be asked to complete a research project involving a current infrastructure problem. Graduate students' projects would include description of the problem, proposed solution alternatives and a comparative evaluation of the solutions. Undergraduate student projects will involve a case study on a selected infrastructure system or issue. Our final deliberations resulted in the course structure diagrammed in Figure 1.

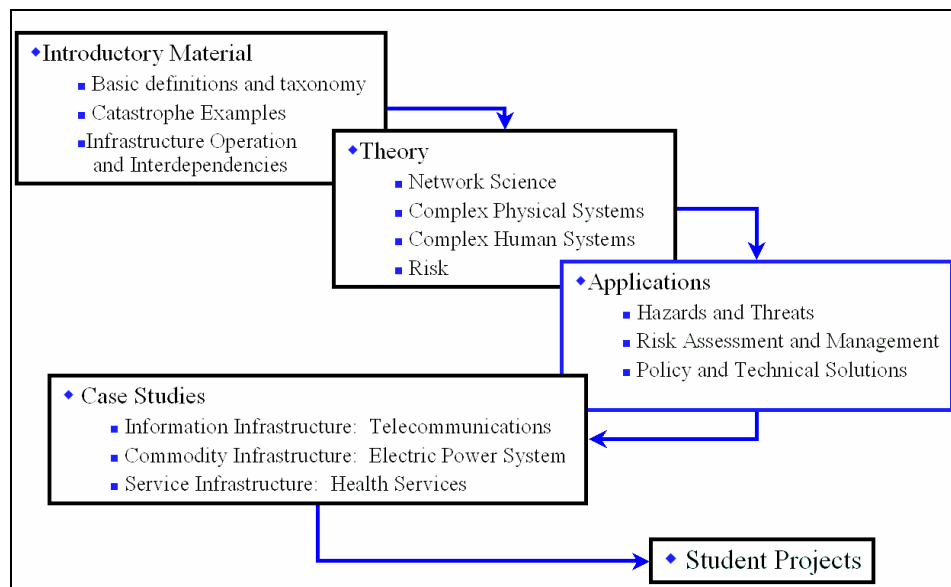


Figure 1: Course Structure

Initial Offering

The course was first offered as a 3-hour experimental course in the fall semester, 2003. Despite our fears of no-to-low enrollment, ten students signed up with an even balance between graduate and undergraduate participants. This class size and mix proved ideal for our initial experiment. We were pleased with the enthusiastic student participation in the course. Class discussions were very lively and turned out to be major part of the learning experience for both students and faculty. Topics that generated heated discussion included risk perception, the relative importance of cyber and physical security, and the assigning of responsibility for system failure (organization structure vs human error vs machine failure vs combinations) In addition, we were able to attract several well-known guest speakers including Mark Manion (author of the book on system

failures, *Minding the Machines*) and William Graham (former President's Science Advisor and Chairman of the Congressional EMP Commission).

As we proceeded with the course, we included many concurrent news events germane to course material, such as the nuclear plant shut down due to a computer virus, the investigation of the 2003 northeast power blackout, and 9-11 diagnostic reports. We asked each student to prepare a 10-minute briefing on a current event related to a complex system failure and consequences. These proved very instructive in relating course principles to actual problems.

We arranged three infrastructure site visits, including the local municipal electric power company, a large local network operations center, and a local food processing plant. During each visit, students received a briefing on site mission from our hosts. And were asked to look for single-point vulnerabilities in site mission and support equipment. Students found these visits to be very beneficial in terms of understanding the ease with which large systems can be disrupted. The actual, week-by-week course progression is presented in Table 1.

Table 1 – Final Course Progression	
UNIT I – Course introduction, critical infrastructure systems	
Week 1	Course introduction
	Catastrophic system failure examples
	Guest lecturer: Richard Little
Week 2	Critical infrastructure taxonomy
	Definitions of common terms
	Infrastructure assurance issues
Week 3	Critical infrastructure design, operation
	Critical infrastructure services
Week 4	Infrastructure interdependencies
	The “vulnerability of complexity”
	Guest lecturer: Mark Manion
UNIT II – Complex Systems Characteristics	
Week 5	Complex system theory
	Modeling complexity
	Example applications
Week 6	Complex systems' social dimensions
	Organizational complexity
	Modeling/simulation of social complexity
UNIT III – Risk	
Week 7	Risk concepts
	Risk perception
	Risk Issues
Week 8	Risk evaluation, metrics
	Fault trees and event trees
	Risk assessment methodology
UNIT IV – Hazards and Threats	
Week 9	Transnational threats

	Biological/genetic threat example
UNIT V – Risk Management	
Week 10	Risk management strategies for infrastructure systems
	Risk management policy and organizations (federal, state, local)
UNIT VI – Case Studies	
Week 11	Telecommunication systems: Guest lecturer Michael Woolman (campus telecommunications manager)
	Data network systems: Guest lecturer Brad Saul (campus computer network manager)
	Information assurance risks and the internet
Week 12	Blackout 2003
	The Challenger disaster
Week 13	Public health system organization and issues, guest lecturer David Cockley, Professor of Public Health
	Dark Winter video presentation, class discussion
	Infrastructure system assessment methodology and lessons learned
UNIT VII – Student Research Project Presentations	Student presentation titles:
Week 14	Civilian Airline Protection
	Risk Assessment of the Blackboard Software System
	The Effects and Implications of Nuclear EMP
	The Effects of Hurricane Isabel on the Virginia Beach Area
Week 15	Vulnerabilities of U.S. Private Industry to Cyber Attacks and Cyber Crime
	Risk Assessment of the Water Supply Infrastructure
	Critical Issues and Risk Analysis of the Water Utility
	Case History of the California Electrical Infrastructure Problems After Deregulation

Course Evaluation

The initial offering of the course received highly favorable feedback from students on their standard evaluation forms. Student written comments reflected satisfaction with the relevance of the course to current societal problems. They felt our team teaching concept using experts in several relevant disciplines worked well. Students were impressed with the amount and variety of information covered. Because the course broadened their perspective on critical needs in the area of homeland security, students felt it helpful to their career decisions and job search. Other positive feedback included appreciation for our use of guest speakers. They cited infrastructure site visits as an important component of the course and our strong emphasis on the relationship of course material to current events and issues.

Students also suggested several ways to improve the course. We received a suggestion for more class discussion time. Because of the volume of reading material, students felt it would be good to provide a bound volume or CD containing the required reading. While students generally liked the broad topics covered, several felt it would be better to split the course to enable more in-depth treatment of the subject matter. One student inquired about the possibility of a lab component incorporating real infrastructure site assessments. Integrated Science and Technology (ISAT) majors felt that the course was extremely relevant. It was recommended that the course should be the basis for a new ISAT concentration area.

Summary and Future Directions

A survey course on critical infrastructure systems has been successfully developed and taught at James Madison University for the past three years.¹⁵ The course is designed for a broad student audience, including physical science, public administration, health, business, economics and sociology majors. We typically enroll 12 students per class, roughly 2/3 graduate students, 1/3 undergraduate. In addition to highly positive student response, the course has piqued the interest of faculty members, and we have had as many as eight instructors involved, each teaching a class related to their specialty area.

The course takes an interdisciplinary approach to understanding complex system operation and failure. We begin by considering historical examples of major system failures. We then explore the components, operation, and complex interdependencies of the infrastructures most critical to society. We divide

¹⁵ The course has been approved as a regular catalog course, ISAT 560.

critical infrastructures into three classes – commodity, service, and information – and focus on the electric power, health services and telecommunication sectors.

Students are exposed to literature that informs their understanding of large, complex, and sometimes risky technical systems. The course emphasizes that complex systems engender unexpected interactions of failures to occur that can result in a cascade of increasingly serious disturbances often culminating in disaster. A major component of the course is devoted to defining and measuring risk. The final instruction block is devoted to risk management strategies involving both technology and public policy. The course concludes with the presentation of student projects that may address a historical complex system failure case study, an assessment of an existing infrastructure system, or survey a specific topic on complex system operation and failure.

The course has been recognized as relevant as part of ongoing and future university curricula initiatives and is part of a new information analyst curriculum presently under development. The success of the course and expansive homeland security objectives in the field of critical infrastructure (as stated in recent national policy documents) presage the possibility of developing an infrastructure assurance curriculum. The Integrated Science and Technology degree program at James Madison University with its existing concentrations in several infrastructure sectors¹⁶ is well suited to providing the home for such a curriculum.

References

Augustine, Norman R., Augustine's Laws, 6th Edition, AIAA Press, 1997.

Axelrod, R. and Cohen, M.D., Harnessing Complexity: Organizational Implications of a Scientific Frontier, Basic Books, New York, N.Y., 2000.

Bak, P. and M. Paczuski, "Complexity, contingency, and criticality", Proceedings of the National Academy of Sciences, National Academy Press, Washington, D.C., pp. 6689-6696, 1995.

Albert, Reka and Barabási, Albert-László "Statistical Mechanics of Complex Systems," Reviews of Modern Physics, Vol 74, January 2002.

Baker, G. H., "A Vulnerability Assessment Methodology for Critical Infrastructure Facilities," Critical Infrastructure Protection Program Workshop Proceedings, George Mason University Press, 2004.

¹⁶ Applicable ISAT concentrations include Telecommunications, Energy, Environment, Information and Knowledge Management, Engineering and Manufacturing, and Biotechnology.

Baker, G. H., et al, "Application of Underground Structures for the Physical Protection of Critical Infrastructure," North American Tunneling Proceedings, 2002. ISBN 90 5809 376 X.

Bar-Yam, Yaneer, Dynamics of Complex Systems, Westview Press, 1997

Branscomb, Lewis M, Klausner, Richard D. et al, Making the Nation Safer: The Role of Science and Technology in Countering Terrorism, National Academies Press, 2002.

Bugliarello, George, Ed., Urban Security: Engineering the Protection of Our Cities, Urban Security Initiative, Polytechnic University, 2002.

Cordesman, Anthony H., Cyber-threats, Information Warfare, and Critical Infrastructure Protection: Defending the U.S. Homeland (Praeger Publishers 2002).

Couch, Richard, The U.S. Armed Forces Nuclear, Biological and Chemical Survival Manual, Perseus Books, 2003

Emerson, Steve, American Jihad.

Garrett, L. 2000. Betrayal of Trust: The Collapse of Global Public Health. New York, N.Y.: Hyperion Books

Garcia, Mary Lynn, The Design and Evaluation of Physical Protection Systems (Butterworth-Heinemann Publishers 2001)

Hammond, K., J. Rohrbaugh, J. Munpower, and L. Adelman. 1977. "Social Judgment Theory: Applications in Policy Formation" in Kaplin and Schwartz (eds.), Human Judgment and Decision Processes in Applied Settings. Academic Press. New York.

Hyndman, Donald, David, Natural Hazards and Disasters, Thomson-Brooks/Cole Publishers, 2006.

Isaacs, Skip, Threats to Symbols of American Democracy, Critical Incident Analysis Group, University of Virginia, 2000.

IOM (Institute of Medicine). To Err Is Human: Building A Safer Health System. Washington, D.C.: National Academy Press, 2000.

Klinenberg, E. 2003. "Victims of a hot climate and a cold society." International Herald Tribune.

Klinenberg, Eric, New York University, Heat Wave: A Social Autopsy of Disaster in Chicago (University of Chicago Press, 2002)

Linstone, H., 1984. Multiple Perspectives for Decision Making: Bridging the Gap Between Analysis and Action. New York, N.Y.:Elsevier-Science Publications.

Little, R.G. et al, Use of Underground Facilities to Protect Critical Infrastructures, National Research Council, 1998

Little, R. 2002. Controlling Cascading Failure: Understanding the Vulnerabilities of Interconnected Infrastructure. *Journal of Urban Technology*. 9(1):109-123.

Little, R., 2004. The Role of Organizational Culture and Values in the Performance of Critical Infrastructure Systems. Proceedings of the 2004 IEEE International Conference on Systems, Man, and Cybernetics. October 10-13, 2004, The Hague, The Netherlands.

Marburger, J. 2002. Testimony before the House Committee on Science. June 14, 2002.

Perrow, C. 1999. Normal Accidents: Living with High-Risk Technologies. Princeton, N.J.: Princeton University Press.

Strieber, Whitley and Kunetka, James W., Warday (Holt, Rinehart and Winston, 1984)

Vaughan, Diane, The Challenger Launch Decision: Risky Technology, Culture, and Deviance at NASA (University of Chicago Press, 1996)

Wagner-Pacifici, Robin, Theorizing the Stand-Off: Contingency in Action (Cambridge University Press, 2000)

Walker, J. Samuel, Three Mile Island: A Nuclear Crisis in Historical Perspective (University of California Press)

Watts, Duncan J., Six Degrees: The Science of a Connected Age, W.W. Norton & Co., 2003.

Wilson, James Q., Bureaucracy (Basic Books, 1989)

Waugh, William L., Living with Hazards, Dealing with Disasters: An Introduction to Emergency Management (M.E. Sharpe Publishers 2002)

Government Publications

Critical Foundations: Protecting America's Infrastructures, The Report of the President's Commission on Critical Infrastructure Protection, 1997.

The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets, U.S. Government Printing Office, 2003

The National Strategy to Secure Cyberspace, U.S. Government Printing Office, 2003.

The National Infrastructure Protection Plan, U.S. Government Printing Office, 2005.

Survival, Department of the Army Field Manual, FM 21-76, 1970.