

Section 6 - Securing Critical Infrastructure and Cyberspace

33. Introduction - James F. McDonnell

34. Critical Infrastructures and their Interdependencies - Rae Zimmerman

1. D. Henry and J. Dumagen, "Economics"; in R. Zimmerman and T.A. Horan (eds.), *Digital Infrastructures: Enabling Civil and Environmental Systems through Information Technology* (London: Routledge, 2004), p. 155.

2. U.S. Department of Commerce, Bureau of Economic Analysis, table 3.1ES, *Current-Cost Net Stock of Private Fixed Assets by Industry, 2001*,

www.bea.gov

. See also J. P. Gould and A.C. Lemer (eds.), *Toward Infrastructure Improvement: An Agenda for Research* (Washington, D.C.: National Academy Press, 1994).

3. A. Altshuler, "Infrastructure Investment"; (Book Review), *Journal of Policy Analysis and Management* 8 (1989): 506. See also D. C. Perry, "Building the Public City: An Introduction"; in D. C. Perry (ed.), *Building the Public City. The Politics, Governance, and Finance of Public Infrastructure* (Thousand Oaks, Calif.: Sage, 1995), pp. 1-20.

4. S. M. Rinaldi, J. P. Peerenboom, and T. K. Kelly, "Identifying, Understanding, and Analyzing Critical Infrastructure Interdependencies"; *IEEE Control Systems* (December 2001): 12.

5. U.S. Executive Office of the President, "The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive 63"; (22 May 1998).

6. T. D. O'Rourke, Y. Wang, and P. Shi, "Advances in Lifeline Earthquake Engineering"; *Proceedings of the Thirteenth World Conference on Earthquake Engineering* (Vancouver, Calif.) (1-6 August 2004).

7. R. Prieto, "The 3Rs: Lessons Learned from September 11"; presented at the Royal Academy of Engineering, 2002.

8. Op. cit.

9. R. Zimmerman, "Planning and Administration: Frameworks and Case studies"; in John Ingleton (ed.), *Natural Disaster Management* (Leicester: Tudor Rose, 1999), pp. 225-7.

10. P. Choate and S. Walter, *America in Ruins* (Durham, N.C.: Duke University Press, 1983).

11. North American Electric Reliability Council (NERC), "Examples of Major Bulk Electric System Power Outages"; n.d.;

<ftp://www.nerc.com>

, accessed 26 September 2004.

12. American Society of Civil Engineers (ASCE), Scorecard: 2003 Progress Report. Washington, D.C.: ASCE, 2003; <http://www.asce.org/reportcard/>, accessed 13 January 2004.
13. National Research Council (NRC), Making the Nation Safer: The Role of Science and Technology in Countering Terrorism (Washington, D.C.: National Academy Press, 2002).
14. Mineta International Institute for Surface Transportation Policy Studies, Protecting Surface Transportation Systems and Patrons from Terrorist Activities (Washington, DC: Mineta Institute, 1997), p. 23.
15. "Tampering Blamed for Power Outage," USA Today (12 October 2004): 3A.
16. R. Zimmerman, "Water," in R. Zimmerman and T. Horan (eds.), Digital Infrastructures: Enabling Civil and Environmental Systems through Information Technology (London: Routledge, 2004a), p. 80.
17. A. S. Khan, D. L. Swerdlow, and D. D. Juranek, "Precautions against Biological and Chemical Terrorism Directed at Food and Water Supplies," Public Health Reports 116 (2001): 7.
18. P. Cachia, "Saboteur Contaminates Water Supply at Ta' Kandja," di-ve news (10 November 2003), <http://www.di-ve.com/dive/portal/portal.jhtml?id%2F114070&pid%2Fnull> (link not current), accessed 4 December 2003. See also Zimmerman, 2004a.
19. U.S. General Accounting Office (GAO), "Critical Infrastructure Protection: Challenges and Efforts to Secure Control Systems," GAO-04-354 (25 April 2004), p. 17.
20. Mineta Institute, 1997.
21. R. Zimmerman, "Social Implications of Infrastructure Network Interactions," in Sustaining Urban Networks: The Social Diffusion of Large Technical Systems (London: Routledge, 2005), p. 69.
22. Op. cit., 2001.
23. R. Zimmerman, "Decision-Making and the Vulnerability of Critical Infrastructure," Proceedings of IEEE International on Systems, Man, and Cybernetics (2004b).
24. Op. cit., 2001, p. 22.
25. Zimmerman, 2005.
26. T. D. O'Rourke, "Prospectus for Lifelines and Infrastructure Research," in B. Stenquist (ed.), The Art and Science of Structural Engineering: Proceedings of the Symposium Honoring William J. Hal (Upper Saddle River, N.J.: Prentice-Hall, 1993), 37-58.
27. R. Zimmerman, "Public Infrastructure Service Flexibility for Response and Recovery in the September 11th, 2001, Attacks at the World Trade Center," in Natural Hazards Research and Applications Information Center, Public Entity Risk Institute, and Institute for Civil Infrastructure Systems, Beyond September 11th: An Account of

Post-Disaster Research, Special Publication 39 (Boulder: University of Colorado, 2003a), pp. 241–268.

28. NRC, *The Internet under Crisis Conditions: Learning from September 11* (Washington, D.C.: National Academy Press, 2003).

29. U.S. Environmental Protection Agency (EPA), *Development, Community, and Environment—Our Built and Natural Environments* (Washington, D.C.: EPA, November 2000).

30. R. Zimmerman and T. Horan (eds.), *Digital Infrastructures: Enabling Civil and Environmental Systems through Information Technology* (London: Routledge, 2004); see the editors’ article ‘‘What Are Digital Infrastructures?’’ p. 71.

31. Cellular Telecommunications and Internet Association (CTIA), ‘‘Semiannual Wireless Industry Survey’’ (Washington, D.C.: CTIA, 2003). See also Zimmerman, 2005, p. 71.

32. D. Bart, Presentation for the Defense Standardization Program Conference: An Update on ANSI Homeland Security Standards Panel (HSSP), ANSI-HSSP, Private Sector Cochair (17 March 2004).

33. Statistics are from, or were calculated from, the following: Zimmerman, 2004b, p. 81: U.S. Bureau of the Census, 1997,

<http://www.census.gov/prod/www/abs/manu-geo.html>

, accessed 29 October 2004; U.S. Department of Energy, Energy Information Administration (DOE, EIA), 2000,

<http://www.eia.doe.gov/cneaf/electricity/ipp/html1/ippv1te1p1.html>

, accessed 29 October 2004; D. Shrank

and T. Lomax, *The 2004 Urban Mobility Report* (College Station: Texas A&M University, Texas Transportation Institute, 2004), p. 71; and U.S. Department of Transportation (DOT), National Transit Database.

34. Mineta Institute, 1997.

35. R. Clemen and T. Reilly, *Making Hard Decisions with Decsiontools* (Pacific Grove, Calif.: Duxbury, 2001), pp. 67–8.

36. GAO, ‘‘Critical Infrastructure Protection: Significant Challenges Need to Be Addressed,’’ GAO-02-961T (24 July 2002), p. 14.

37. Y. Haimes and P. Jiang, ‘‘Leontief-Model of Risk in Complex Interconnected Infrastructures,’’ *Journal of Infrastructure Systems* 7:1 (2001): 1–12.

38. Op. cit.

39. A. Rose, J. Benavides, S. Chang, P. Szczesniak, D. Lim, ‘‘The Regional Economic Impact of an Earthquake: Direct and Indirect Effects of Electricity Lifeline Disruptions,’’ *Journal of Regional Science* 37:3 (1997): 437–58.

40. H. Martz and M. Johnston, ‘‘Risk Analysis of Terrorist Attack,’’ *Risk Analysis* 7 (1987): 35–47.

41. E. Pate-Cornell, "Probabilistic Modeling of Terrorist Threats: A System Analysis Approach to Setting Priorities Counter Measures," *Military Operations Research* 7:4 (December 2002): 5-20.
42. O'Rourke, Wang, and Shi, 2004.
43. G. Apostolakis, "The Concept of Probability in Safety Assessments of Technological Systems," *Science* 250:7 (7 December 1990).
44. Y. Haimes, *Risk Modeling, Assessment and Management* (New York: Wiley, 2004).
45. B. Ezell, J. V. Farr, and I Wiese, "Infrastructure Risk Analysis Model" and "Infrastructure Risk Analysis of Municipal Water Distribution System," *Journal of Infrastructure Systems* 6:3 (2000): 114-17, 118-22.
46. M. Leung, J. H. Lambert, and A. Mosenthal, "A Risk-Based Approach to Setting Priorities in Protecting Bridges against Terrorist Attacks," *Risk Analysis* 24:2 (2004): 963-84.
47. L. Mili, Q. Qiu, and A. G. Phadke, "Risk Assessment of Catastrophic Failures in Electric Power Systems," *International Journal of Critical Infrastructures* 1:1 (2004): 38-63.
48. B. Fischhoff, P. Slovic, S. Lichtenstein, S. Read, and B. Combs, "How Safe Is Safe Enough: A Psychometric Study of Attitudes toward Technological Risks and Benefits," in P. Slovic (ed.), *The Perception of Risk* (London and Sterling, Va.: Earthscan, 2000): 80-103.
49. B. Fischhoff, "Assessing and Communicating the Risks of Terrorism," in A. H. Teich, S. D. Nelson, and S. J. Lita (eds.), *Science and Technology in a Vulnerable World* (Washington, D.C.: AAAS, 2002): 51-64. See also B. Fischhoff, R. M. Gonzalez, D. A. Small, and J. S. Lerner, "Evaluating the Success of Terror Risk Communications," *Biosecurity and Bioterrorism: Biodefense Strategy, Practice, and Science* 1 (2003): 255-8.
50. Zimmerman, 2004a.
51. GAO, 2002, p. 17.
52. *Ibid.*, p. 26.
53. *Ibid.* For more detail, see also National Academy of Engineering, Computer Science, and Telecommunications Board (CSTB), *Critical Information Infrastructure Protection and the Law: An Overview of Key Issues* (Washington, D.C.: National Academy Press, 2003).
54. GAO, 2004, p. 27.
55. TheOrator.com,
http://www.theorator.com/bills108/issues/homeland_security.html
 , accessed 30 October 2004.

56. GAO, 2002, p. 10.

57. National Commission on Terrorist Attacks upon the United States, *The 9/11 Commission Report* (New York: Norton, 2004).

58. K. G. Herron and H. C. Jenkins-Smith, *U.S. Public Response to Terrorism: Panel Study 2001–2002* (College Station: Texas A&M University, August 2003), pp. 3,

22–8; table 2.5.

59. Zimmerman and Horan, 2004, p. 6.

60. Henry and Dumagan, *op. cit.*

61. E.g., Zimmerman and Horan, 2004; NRC, 2002, 2003.

62. GAO, 2004, pp. 6, 12.

63. Electricity Consumers Resource Council, ‘’The Economic Impacts of the August 2003 Blackout’’ (2 February 2004).

64. U.S.-Canada Power System Outage Task Force, *Final Report on the August 14th 2003 Blackout in the United States and Canada: Causes and Recommendations* (April 2004).

65. R. Zimmerman, ‘’NYC Needs Systems to Blunt New Blackouts,’’ *Newsday* (27 August 2003b): A31.

66. R. Truly, ‘’New Energy Systems Enhance National Security,’’ DOE, National Renewable Energy Laboratory, 14 March 2002; http://www.nrel.gov/director/trulyspeech_031402.html (link not current).

67. U.S. Department of Energy, Energy Information Administration (DOE/EIA), *Renewable Energy Trends 2003* (Washington, D.C.: July 2004): 1–2.

68. C. Lenatti, ‘’Nanotech’’s First Block-busters,’’ *Technology Review*(March2004): 46–52.

69. DOE/EIA, *op. cit.*, p. 6.

35. *Cyber Security in Post 9/11 America* - James Cunningham

1. Mosaic was developed by a team at the National Center for Supercomputing Applications at the University of Illinois, Urbana-Champaign (NCSA-UIUC) by Marc Andreessen and Eric Bina. (Spyglass acquired their technology from NCSA.)

2.

www.isc.org/ops/ds/reports/2004-01/

.

3. History of ARPANET, Part IV: Conclusion,

www.dei.isep.ipp.pt/docs/arpa–4.html

.

4. Definitions were adapted from How Computer Viruses Work by Marshall Brain,

<http://computer.howstuffworks.com/virus.html>

.

5. CERT/CC is a center of Internet security expertise at Carnegie Mellon University's Software Engineering Institute. See www.cert.org.

6. Derived from CERT Advisory CA-2004-02 E-mail-borne Viruses,

www.cert.org/advisories/CA-2004-02.html

.

7. www.deloitte.com/dtt/research/0,2310,sid%41013&cid%448978,00.html (link not current).

8. Alan Cullison, 'Inside al-Qaeda's Hard Drive,' Atlantic (November 2004).

9. David Bamber, 'Bin Laden: Yes, I Did It,' news.telegraph.co.uk, 11 November 2001;

www.portal.telegraph.co.uk/news/main.jhtml?xml%4/news/2001/11/11/wbin11.xml

.

10. These scenarios almost always involve the electronic hijacking of supervisory control and data acquisition (SCADA) systems connected to a data network via a wide area network. The sophistication of SCADA systems and their associated distributed control systems (DCSs) varies widely. But modern SCADA and DCS systems operate metropolitan water distribution networks, major water and

wastewater treatment plants, and wastewater collection systems.

11. Dial-up connections to individual computers and to internal (private) networks for diagnostic and repair pose an entirely separate set of potential vulnerabilities.

12. Most DNS data needed to pass communications are stored locally and updated daily. Very few name resolution requests require root server assistance.

13. Internet Society, A Brief History of the Internet,

www.isoc.org/internet/history/brief.shtml

.

14. The former Critical Infrastructure Assurance Office, the National Infrastructure Protection Center, the Federal Computer Incident Response Center, and the National Communications System were transferred to DHS to become the nucleus of NCSD.

15. Progress and Challenges in Securing the Nation's Cyberspace, Department of Homeland Security Office of the Inspector General, OIG-04-29 (July 2004).

16. George V. Hulme and Stephanie Stahl, 'Q&A with Amit Yoran'; Information Week 13 (February 2004).

17. Federal guidelines for protecting information are found in the Federal Information Management Act of 2002 (FISMA):

<http://csrc.nist.gov/policies/FISMA-final.pdf>

.

18. William New, 'Homeland Security Has No Plans to Update Cybersecurity Strategy'; National Journal's Technology Daily (10 June 2004).

19.

www.computerworld.com/printthis/2004/0,4814,91899.00.html

.

20. The National Strategy to Secure Cyberspace (February 2003), p. viii,

www.whitehouse.gov/pcipb/

.

21. William New, 'Ex-Cybersecurity Czar Blasts Bush's Efforts'; National Journal's Technology Daily (17 May 2004).

22. National Institute of Standards and Technology, Computer Security Resource Center (NIST CSRC),

<http://csrc.nist.gov/>

.

23. National Security Agency's Infrastructure Assurance Directorate (NSA IAD),

www.nsa.gov/ia/

24. Policies for handling information include how documents are created, revised, published, temporarily stored, archived, and destroyed. Policy for information security deals with information assets and how to ensure their confidentiality, integrity, and availability. Policies are high-level statements of broad intent, such as “Product development data will be protected at all times.” Standards are used to interpret policies for individual departments and users and are typically written in plain, straightforward terms. Guidelines tend to be technical

implementation rules.

25. National Strategy to Secure Cyberspace, p. 11.