References

1. D.H. Meadows, *Thinking in Systems: A Primer*, Chelsea Green Publishing, 2008.
2. J.P. Crutchfield, "The Hidden Fragility of Complex Systems—Consequences of Change, Changing Consequences," in *Cultures of Change: Social Atoms and Electronic Lives*, edited by G. Ascione, C. Massip, and J. Perello, Actard Publishers, 2009, pp. 98–111.
3. D. Helbing, "Systemic Risks in Society and Economics," SFI Working Paper 2009-12-044, 2009, www.santafe.edu/media/workingpapers/09-12-044.pdf.
4. D. Helbing, "Globally Networked Risks and How to Respond," *Nature*, vol. 497, 2013, pp. 51–59.
5. S.M. Rinaldi, J.P. Peerenboom, and T.K. Kelly, "Identifying, Understanding, and Analyzing Critical Infrastructure Interdependencies," *IEEE Control Systems*, vol. 21, no. 6, 2001, pp. 11–25.
6. R.G. Little, "Controlling Cascading Failure: Understanding the Vulnerabilities of Interconnected Infrastructures," *Journal of Urban Technology*, vol. 9, no. 1, 2002, pp. 109–123.
7. K.J. Hole, "Management of Hidden Risks," *IEEE Computer*, vol. 46, no. 1, 2013, pp. 65–70.
8. N.N. Taleb, *Fooled by Randomness: The Hidden Role of Chance in Life and in the Markets*, 2nd edition, Random House, 2005.
9. N.N. Taleb, *The Black Swan: The Impact of the Highly Improbable*, 1st edition, Random House, 2007. See also the 2nd edition from 2010 with a new essay on robustness and fragility.
10. N.N. Taleb, *Antifragile: Things That Gain from Disorder*, Random House, 2012.
11. N.N. Taleb, "The Fourth Quadrant: A Map of the Limits of Statistics," Edge, 14 September 2008.
12. N.N. Taleb, R. Read, R. Douady, J. Norman, and Y. Bar-Yam, "The Precautionary Principle (with Application to the Genetic Modification of Organisms)," 2014, arxiv.org/abs/1410.5787.
13. M.J. Kavis, *Architecting the Cloud*, Wiley, 2014.
14. B. Wilder, *Cloud Architecture Patterns*, O'Reilly, 2012.
15. C. Perrow, *Normal Accidents: Living with High-Risk Technologies*, Princeton University Press, 1999.
16. J.H. Miller and S.E. Page, *Complex Adaptive Systems*, Princeton University Press, 2007.
17. S. Dekker, *Drift into Failure*, Ashgate, 2011.
18. S. Dekker, *Safety Differently*, 2nd edition, CRC Press, 2014.
19. S. Robinson and M.M. Robinson, *Holonomics*, Floris Books, 2014.
20. C. Gros, *Complex and Adaptive Dynamical Systems*, Springer, 2008.
21. C.C. Elisan, *Malware, Rootkits & Botnets*, McGraw-Hill Osborne Media, 2012.
22. Q. Li and G. Clark, "Mobile Security: A Look Ahead," *Security & Privacy*, vol. 11, no. 1, 2013, pp. 78–81.
23. M.E.J. Newman, *Networks: An Introduction*, Oxford University Press, 2010.

K.J. Hole, *Anti-fragile ICT Systems*, Simula SpringerBriefs on Computing 1,
DOI 10.1007/978-3-319-30070-2

24. M. Franz, "E Unibus Pluram: Massive-Scale Software Diversity as a Defense Mechanism," *Proceedings of the New Security Paradigms Workshop 2010*, Concord, MA, 21–23 September 2010, pp. 7–16.
25. R. Cohen, S. Havlin, and D. Ben-Avraham, "Efficient Immunization Strategies for Computer Networks and Populations," *Physical Review Letters*, vol. 91, no. 24, Article ID 247901, 2003.
26. D. Montague, *Essentials of Online Payment Security and Fraud Prevention*, Wiley, 2011.
27. J. Hawkins and S. Blakeslee, *On Intelligence*, Times Books, 2004.
28. D.E. Geer, "Monopoly Considered Harmful," *IEEE Security & Privacy*, vol. 1, no. 6, 2003, pp. 14–17.
29. D.E. Geer, "Monoculture on the Back of the Envelope," *;login:*, vol. 30, no. 6, 2005, pp. 6–8.
30. D.E. Geer, "Dan Geer Keynote," Source 2008 Conference, Boston, MA, 13 March 2008, http://geer.tinho.net/geer.sourceboston.txt.
31. D.E. Geer, "Dan Geer Keynote," Source 2012 Conference, Boston, MA, 18 April 2012, http://geer.tinho.net/geer.sourceboston.18iv12.txt.
32. D.E. Geer, "Complexity Is the Enemy," *IEEE Security & Privacy*, vol. 6, no. 6, 2008, p. 88.
33. D. E. Geer, "People in the Loop: Are They a Failsafe or a Liability?" Suits & Spooks, 8 February 2012, http://tinyurl.com/7cavobr.
34. K.J. Hole and L.-H. Netland, "Toward Risk Assessment of Large-Impact and Rare Events," *IEEE Security & Privacy*, vol. 8, no. 3, 2010, pp. 21–27.
35. M.T. Nygard, *Release It!* Pragmatic Bookshelf, 2007.
36. D. Kahneman, *Thinking, Fast and Slow*, Farrar, Straus and Giroux, 2011.
37. J. Humble, J. Molesky, and B. O'Reilly, *Lean Enterprise*, O'Reilly Media, 2015.
38. D. Zwieback, "Antifragile Systems and Teams," O'Reilly Media, 2014.
39. P. Triana, *Lecturing Birds on Flying: Can Mathematical Theories Destroy the Financial Markets?* Wiley, 2009.
40. B. Mandelbrot and R.L. Hudson, *The (Mis)behavior of Markets: A Fractal View of Financial Turbulence*, annotated edition, Basic Books, 2006.
41. A. Tseitlin, "The Antifragile Organization," *Communications of the ACM*, vol. 56, no. 8, 2013, pp. 40–44.
42. S.C. Currall and M.J. Epstein, "The Fragility of Organizational Trust: Lessons From the Rise and Fall of Enron," *Organizational Dynamics*, vol. 32, no. 2, 2003, pp. 193–206.
43. L.H. Nestås and K.J. Hole, "Building and Maintaining Trust in Internet Voting," *IEEE Computer*, vol. 45, no. 5, 2012, pp. 74–80.
44. E.A. Whitley and G. Hosein, *Global Challenges for Identity Policies*, Palgrave Macmillan, 2010.
45. E. Pieri, "ID Cards: A Snapshot of the Debate in the UK Press," project report, ESRC National Centre for e-Social Science, University of Manchester, 2009.
46. U. Wilensky, NetLogo, Center for Connected Learning and Computer-Based Modeling, Northwestern University, Evanston, IL, 1999, https://ccl.northwestern.edu/netlogo.
47. G.S. Lynch, *Single Point of Failure*, Wiley, 2009.
48. L. Bass, P. Clements, and R. Kazman, *Software Architecture in Practice*, 3rd edition, Addison-Wesley, 2012.
49. P. Csermely, *Weak Links*, Springer, 2006.
50. S.E. Page, *Diversity and Complexity*, Princeton University Press, 2010.
51. Y. Bar-Yam, "The Limits of Phenomenology: From Behaviourism to Drug Testing and Engineering Design," New England Complex Systems Institute (NECSI) Report 2013-08-01, arxiv.org/abs/1308.3094.
52. M. Richards, *Software Architecture Patterns*, O'Reilly Media, 2015.
53. S. Newman, *Building Microservices*, O'Reilly Media, 2015.
54. L. Krause, *Microservices: Patterns and Applications*, Amazon Digital Services, 2015.
55. P.J. Sadalage and M. Fowler, *NoSQL Distilled: A Brief Guide to the Emerging World of Polyglot Persistence*, Addison-Wesley, 2012.
56. K.J. Hole, "Diversity Reduces the Impact of Malware," *IEEE Security & Privacy*, vol. 13, no. 3, 2015, pp. 48–54.

57. Det Norske Veritas, "Vurdering av Altinn II-platformen," report in Norwegian commissioned by the Norwegian Ministry of Trade and Industry, version 1.1, 2012.
58. Capgemini Norge, "Altinn—en plattform å satse på?" report in Norwegian commissioned by the Norwegian Ministry of Trade and Industry, 2012.
59. Ministry of Government Administration, Reform and Church Affairs, "Digitizing Public Sector Services," Norwegian eGovernment Program, 2012, https://www.regjeringen.no/en/dokumenter/digitization-public-sector-services/id698435.
60. Government ministers Karl Eirik Schjøtt-Pedersen and Rigmor Aasrud discussed the effort to digitalize Norway's public sector, Digitaliseringskonferansen, Oslo, Norway, 30–31 May 2012.
61. Video by The Guardian, "How Geeks Opened up Government," 2013, www.guardian.co.uk/technology/video/2013/jun/13/geeks-opened-up-government-video.
62. K.J. Hole, "Building Trust in E-Government Services," *IEEE Computer*, vol. 49, no. 1, 2016, pp. 66–74.
63. P. Rost, C.J. Bernardos, A. De Domenico, M. Di Girolamo, M. Lalam, A. Maeder, D. Sabella, and D. Wübben, "Cloud Technologies for Flexible 5G Radio Access Networks," *IEEE Communications Magazine*, vol. 52, no. 5, 2014, pp. 68–76.
64. M.S. Dayananda and J. Priyanka, "Managing Software Defined Radio through Cloud Computing," *Proceedings of the IEEE International Conference on Advanced Communication Control and Computing Technologies*, Ramanathapuram, India, 23–25 August 2012, pp. 50–55.
65. I.R. Lorange, "Hendelsesrapport: Problemer i Telenors mobilnett 10. juni 2011," report from Telenor in Norwegian.
66. Post- og teletilsynet, "Hendelsesrapport: Utfall i Telenors mobilnett 10. juni 2011," report from the Norwegian Post and Telecommunications Authority in Norwegian.
67. I.R. Lorange, "Hendelsesrapport: Problemer i Telenors mobilnett 17. juni 2011," report from Telenor in Norwegian.
68. Post- og teletilsynet, "Hendelsesrapport om utfall i Telenors mobilnett 17. juni 2011," report from the Norwegian Post and Telecommunications Authority in Norwegian.
69. R. Dyrlie, "Hendelsesrapport 2: Problemer i Telenors mobilnett 10. juni 2011," report from Telenor in Norwegian.
70. Post- og teletilsynet, "Foreløpige erfaringer og forslag til tiltak etter ekstremværet Dagmar," report from the Norwegian Post and Telecommunications Authority in Norwegian, 2012.
71. Direktoratet for samfunnssikkerhet og beredskap, "Teknologiskiftet i Telenors infrastruktur," report from the Norwegian Directorate for Civil Protection in Norwegian, 2013.
72. K.J. Hole, O. Lysne, and S. Maharjan, "Consequences of the Trust Relationship between Telecom Operators and Vendors," white paper from Simula Research Laboratory, version 0.9.2, 2014.
73. Post- og teletilsynet, "Hendelsesrapport: Dobbelt fiberbrudd i Telenors nett, 23. mai 2011," report from the Norwegian Post and Telecommunications Authority in Norwegian.
74. "Kost-/nyttevurdering av tiltak for styrking av norsk sambands- og IP-infrastructur," risk analysis in Norwegian by Nexia and Styrmand for the Norwegian Post and Telecommunications Authority.
75. B. Potter, "Necessary but Not Sufficient," *IEEE Security & Privacy*, vol. 8, no. 5, 2010, pp. 57–58.
76. E.M. Hutchins, M.J. Cloppert, and R.M. Amin, "Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains," *Proceedings of the Sixth International Conference on Information Warfare and Security*, Washington, DC, 17–18 March 2011, pp. 113–125.
77. P. Larsen, A. Homescu, S. Brunthaler, and M. Franz, "SoK: Automated Software Diversity," *Proceedings of the 35th IEEE Symposium on Security and Privacy*, San Jose, CA, 18–21 May 2014, pp. 276–291.
78. M. Garcia, A. Bessani, I. Gashi, N. Neves, and R. Obelheiro, "OS Diversity for Intrusion Tolerance: Myth or Reality?" *Proceedings of the 2011 IEEE/IFIP 41st International Conference on Dependable Systems & Networks*, Washington, DC, 27–30 June 2011, pp. 383–394.

79. J. Han, D. Gao, and R.H. Deng, "On the Effectiveness of Software Diversity: A Systematic Study on Real-World Vulnerabilities," *Proceedings of the Sixth International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment*, Milan, Italy, 9–10 July 2009, pp. 127–146.
80. J. Balthrop, S. Forrest, M.E.J. Newman, and M.M. Williamson, "Technological Networks and the Spread of Computer Viruses," *Science*, vol. 304, no. 5670, 2004, pp. 527–529.
81. M. Kitsak, L.K. Gallos, S. Havlin, F. Liljeros, L. Muchnik, H.E. Stanley, and H.A. Makse, "Identification of Influential Spreaders in Complex Networks," *Nature Physics*, vol. 6, no. 11, 2010, pp. 888–893.
82. K.J. Hole, "Toward a Practical Technique to Halt Multiple Virus Outbreaks on Computer Networks," *Journal of Computer Networks and Communications*, vol. 2012, Article ID 462747, December 2012, http://www.hindawi.com/journals/jcnc/2012/462747/.
83. T. Jackson, B. Salamat, A. Homescu, K. Manivannan, G. Wagner, A. Gal, S. Brunthaler, Ch. Wimmer, and M. Franz, "Compiler-Generated Software Diversity," in *Moving Target Defense: Creating Asymmetric Uncertainty for Cyber Threats*, edited by S. Jajodia, A.K. Ghosh, V. Swarup, C. Wang, and X.S. Wang, Springer, 2011, pp. 77–98.
84. K. Kravvaritis, D. Mitropoulos, and D. Spinellis, "Cyberdiversity: Measures and Initial Results," *Proceedings of the 14th Panhellenic Conference on Informatics*, Tripoli, Greece, 10–12 September 2010, pp. 135–140.
85. P. Wang, M.C. González, C.A. Hidalgo, and A.-L. Barabási, "Understanding the Spreading Patterns of Mobile Phone Viruses," *Science*, vol. 324, no. 5930, 2009, pp. 1071–1076.
86. J. Caballero, T. Kampouris, D. Song, and J. Wang, "Would Diversity Really Increase the Robustness of the Routing Infrastructure against Software Defects?" Technical Report CMU-Cylab-07-002, Department of Electrical and Computer Engineering, Carnegie Mellon University, 2008, http://repository.cmu.edu/ece/40/.
87. J.O. Kephart and S.R. White, "Directed-Graph Epidemiological Models of Computer Viruses," *Proceedings of the 1991 IEEE Computer Society Symposium on Research in Security and Privacy*, Oakland, CA, May, 1991, pp. 343–359.
88. J. Maeda, *The Laws of Simplicity*, MIT Press, 2006.
89. P. Larsen, S. Brunthaler, and M. Franz, "Security through Diversity: Are We There Yet?" *IEEE Security & Privacy*, vol. 12, no. 2, 2014, pp. 28–35.
90. K.J. Hole, "Towards Anti-fragility: A Malware-Halting Technique," *IEEE Security & Privacy*, vol. 13, no. 4, 2015, pp. 40–46.
91. K. Salah, J.M. Alcaraz Calero, S. Zeadally, S. Al-Mulla, and M. Alzaabi, "Using Cloud Computing to Implement a Security Overlay Network," *Security & Privacy*, vol. 11, no. 1, 2013, pp. 44–53.
92. E.G. Amoroso, "From the Enterprise Perimeter to a Mobility-Enabled Secure Cloud," *Security & Privacy*, vol. 11, no. 1, 2013, pp. 23–31.
93. M. Abadi, M. Budiu, Ú. Erlingsson, and J. Ligatti, "Control-Flow Integrity Principles, Implementations, and Applications," *ACM Transactions on Information and System Security,* vol. 13, no. 1, 2009.
94. J. Milliken, V. Selis, and A. Marshall, "Detection and Analysis of the Chameleon WiFi Access Point Virus," *EURASIP Journal on Information Security*, vol. 2013, no. 2, 2013.
95. A.-L. Barabási, R. Albert, and H. Jeong, "Scale-Free Characteristics of Random Networks: The Topology of the World-Wide Web," *Physica A*, vol. 281, no. 1–4, 2000, pp. 69–77.
96. Numenta, "Hierarchical Temporal Memory," white paper, version 0.2.1, 2011.
97. R.W. Price, "Hierarchical Temporal Memory Cortical Learning Algorithm for Pattern Recognition on Multi-core Architectures," Master's Thesis, Portland State University, 2011.
98. M. Galetzka, "Intelligent Predictions: An Empirical Study of the Cortical Learning Algorithm," Master's Thesis, Department of Computer Science, University of Applied Sciences Mannheim, 2014.
99. J. Hertz, A. Krogh, and R.G. Palmer, *Introduction to the Theory of Neural Computation*, Addison-Wesley, 1991.
100. J.H. Holland, *Adaption in Natural and Artificial Systems*, MIT Press, 1992.

101. J. Copeland, *Artificial Intelligence: A Philosophical Introduction*, Wiley-Blackwell, 1993.
102. Y. LeCun, Y. Bengio, and G. Hinton, "Deep Learning," *Nature*, vol. 521, 2015, pp. 436–444.
103. J. Fodor, *The Mind Doesn't Work That Way*, MIT Press, 2000.
104. R. Penrose, *The Emperor's New Mind: Concerning Computers, Minds, and the Laws of Physics*, Oxford University Press, 1989.
105. R. Penrose, *Shadows of the Mind: A Search for the Missing Science of Consciousness*, Oxford University Press, 1994.
106. D.J. Chalmers, *The Conscious Mind*, Oxford University Press, 1996.
107. V.B. Mountcastle, "An Organizing Principle for Cerebral Function: The Unit Model and the Distributed System," in *The Mindful Brain*, edited by G.M. Edelman and V.V. Mountcastle, MIT Press, 1978, pp. 7–50.
108. S. Ahmad and J. Hawkins, "Properties of Sparse Distributed Representations and their Application to Hierarchical Temporal Memory," 2015, arxiv.org/abs/1503.07469.
109. Numenta, "The Science of Anomaly Detection," white paper, 2014.
110. Numenta, "Rogue Behavior Detection," white paper, 2014.
111. M. Scheffer, J. Bascompte, W.A. Brock, V. Brovkin, S.R. Carpenter, V. Dakos, H. Held, E.H. van Nes, M. Rietkerk, and G. Sugihara, "Early-Warning Signals for Critical Transitions," *Nature*, vol. 461, 2009, pp. 53–59.
112. D. Sornette, "Dragon-Kings, Black Swans and the Prediction of Crises," 2009, arxiv.org/abs/0907.4290.
113. V. Chandola, A. Banerjee, and V. Kumar, "Anomaly Detection: A Survey," *ACM Computing Surveys*, vol. 41, no. 3, article no. 15, 2009.

Index

K.J. Hole, *Anti-fragile ICT Systems*, Simula SpringerBriefs on Computing 1,
DOI 10.1007/978-3-319-30070-2