

Contents

Part I The Concept of Anti-fragility

1	Introduction	3
1.1	Complex Adaptive Systems	4
1.2	Fragile, Robust, and Anti-fragile Systems	7
1.3	Overview of Book	7
1.4	Creating and Maintaining Anti-fragility	8
1.5	Anti-fragility to Downtime	9
1.6	Anti-fragility to Malware Spreading	9
1.7	Anomaly Detection	10
1.8	Ongoing Explanatory Work	11
2	Achieving Anti-fragility	13
2.1	Black and Gray Swans	13
2.2	Examples of Swans	15
2.3	Limiting the Impact of Failures	16
2.4	Learning from Small Failures	17
2.5	An Alternative Justification	18
2.6	Risk Analyses Ignore Swans	19
2.7	Understanding and Reducing Risk	20
2.8	Taleb’s Four Quadrants	21
2.9	Discussion and Summary	22
3	The Need to Build Trust	25
3.1	Defining Trust	25
3.2	Explanatory Trust Model	27
3.3	Model Limitations	29
3.4	Trust Is Fragile	29
3.5	Distrust Is Robust	31

- 3.6 Maintaining Trust. 32
 - 3.6.1 Prepare Alternative Services 32
 - 3.6.2 Make Digital Services Voluntary 33
 - 3.6.3 Build a Good Track Record. 33
- 3.7 Discussion and Summary 34
- 4 Principles Ensuring Anti-fragility 35**
 - 4.1 Modularity 35
 - 4.2 Weak Links 37
 - 4.3 Redundancy. 37
 - 4.4 Diversity 38
 - 4.5 Fail Fast 39
 - 4.6 Systemic Failure Without Failed Modules 39
 - 4.7 The Need for Models 41
 - 4.8 Discussion. 42
- Part II Anti-fragility to Downtime**
- 5 Anti-fragile Cloud Solutions 47**
 - 5.1 Choice of System Realization 47
 - 5.2 Modularity via Microservices. 49
 - 5.3 Weak Links via Circuit Breakers 49
 - 5.4 Redundancy Provided by the Cloud 50
 - 5.5 Diversity Enabled by the Cloud 52
 - 5.6 Fail Fast Using Software Tools 54
 - 5.7 Top-Down Design and Bottom-Up Tinkering 55
 - 5.8 Discussion and Summary 55
- 6 Toward an Anti-fragile e-Government System 57**
 - 6.1 The Norwegian e-Government System 57
 - 6.2 Redesign Needed 59
 - 6.3 Better Testing 59
 - 6.4 Availability Requirements 60
 - 6.5 Fine-Grained SOA in a Public Cloud 60
 - 6.6 User-Focused and Iterative Development. 61
 - 6.7 Single Versus Multiple Systems. 62
 - 6.7.1 Systems with Strongly Connected Modules 62
 - 6.7.2 Cloud-Based Systems of Weakly Connected
Modules 63
 - 6.8 Discussion and Summary 64
- 7 Anti-fragile Cloud-Based Telecom Systems 67**
 - 7.1 Anti-principles Causing Fragility to Downtime. 68
 - 7.2 Past Fragility to Downtime 68
 - 7.3 Indicators of Fragility to Future Downtime 70
 - 7.4 Robust Access Networks. 73

- 7.5 Robust Network Core 75
- 7.6 Reduced Dependency on the Power Grid 75
- 7.7 Reduced Dependency on One Infrastructure. 76
- 7.8 Anti-fragility to Downtime 76
- 7.9 Discussion and Summary 77

Part III Anti-fragility to Malware

- 8 Robustness to Malware Spreading 81**
 - 8.1 Introduction 81
 - 8.2 Explanatory Epidemiological Model 82
 - 8.2.1 Epidemiological Model 82
 - 8.2.2 Non-predictive Model 83
 - 8.3 Malware-Halting Technique. 84
 - 8.4 Halting Technique Analysis. 85
 - 8.5 Halting Technique Performance 87
 - 8.5.1 Sparse and Homogeneous Networks 87
 - 8.5.2 Dense and Homogeneous Networks 89
 - 8.6 Persistent Targeted Attacks 89
 - 8.7 Related Work 90
 - 8.8 Summary 92
- 9 Robustness to Malware Reinfections 93**
 - 9.1 Malware Attack on a Norwegian Bank 93
 - 9.2 Stochastic Epidemiological Model 94
 - 9.3 How to Immunize Unknown Hubs 95
 - 9.4 Lower Bound on Required Diversity 96
 - 9.5 Discussion and Summary 97
- 10 Anti-fragility to Malware Spreading 99**
 - 10.1 System Model 100
 - 10.1.1 Model Description 101
 - 10.1.2 Model Limitations 102
 - 10.2 Anti-fragility on Static Graphs 103
 - 10.2.1 Simulations of Anti-fragility on Static Networks. 104
 - 10.2.2 Anti-fragility on Large Static Networks. 105
 - 10.3 Anti-fragility on Time-Varying Graphs 105
 - 10.3.1 Simulations of Anti-fragility 106
 - 10.4 Discussion. 109

Part IV Anomaly Detection

- 11 The HTM Learning Algorithm 113**
 - 11.1 The Problem with Classical AI Research. 114
 - 11.2 An Alternative Approach to Learning 114

- 11.3 The Brain’s Neocortex 115
 - 11.3.1 Communication 116
 - 11.3.2 Memory 117
 - 11.3.3 Predictions 117
- 11.4 Overview of HTM 118
 - 11.4.1 Sparse Distributed Representation. 118
 - 11.4.2 Proximal Dendrite Segments 119
 - 11.4.3 Distal Dendrite Segments 120
- 11.5 The Three Steps of HTM 121
 - 11.5.1 Make an SDR of the Input 121
 - 11.5.2 Represent the Input in Context of Previous Inputs 122
 - 11.5.3 Make Prediction from Current and Previous Inputs. . . . 123
- 11.6 Discussion and Summary 124
- 12 Anomaly Detection with HTM 125**
 - 12.1 Anomalies. 125
 - 12.2 HTM Anomaly Score 126
 - 12.3 HTM Anomaly Probabilities 127
 - 12.4 Grok the Cloud 127
 - 12.5 Rogue Behavior. 129
 - 12.6 Detecting the Beginning of Swans 130
 - 12.7 Discussion and Summary 131
- Part V Future Anti-fragile Systems**
- 13 Summary and Future Work 135**
 - 13.1 Achieving Anti-fragility 135
 - 13.2 Future Anti-fragile ICT Systems. 137
 - 13.3 Future Bio-inspired System Designs 138
 - 13.4 The Need for Anti-fragile Processes 139
 - 13.5 Challenge to Readers 140
- References 141**
- Index 147**



<http://www.springer.com/978-3-319-30068-9>

Anti-fragile ICT Systems

Hole, K.J.

2016, XVIII, 151 p. 44 illus., 22 illus. in color., Softcover

ISBN: 978-3-319-30068-9