Louis Anthony Cox, Jr.

# Risk Analysis of Complex and Uncertain Systems



## Contents

¢

#### Part I Introduction to Risk Analysis

1	Quantitative Risk Assessment Goals and Challenges	3
	The Quantitative Risk Assessment (QRA) Paradigm	3
	Example: A Simple QRA Risk Assessment Model	4
	Example: Explicit QRA Reasoning Can Be Checked and Debated	6
	Against QRA: Toward Concern-Driven Risk Management	7
	Dissatisfactions with QRA	7
	Example: Use of Incorrect Modeling Assumptions in Antimicrobial	
	Risk Assessment	8
	Example: Use of Unvalidated Assumptions in a QRA for BSE	
	("Mad Cow" Disease)	9
	Toward Less Analytic, More Pluralistic Risk Management	11
	Alternatives to QRA in Recent Policy Making: Some Practical	
	Examples	13
	Concern-Driven Risk Management	15
	Potential Political Advantages of Concern-Driven Regulatory	
	Risk Management	16
	How Effective Is Judgment-Based Risk Management?	18
	Example: Expert Judgment vs. QRA for Animal Antibiotics	18
	Performance of Individual Judgment vs. Simple Quantitative Models	19
	Performance of Consensus Judgments vs. Simple Quantitative Models	26
	Example: Resistance of Expert Judgments to Contradictory Data	26
	Example: Ignoring Disconfirming Data About BSE Prevalence	28
	Example: Consensus Decision Making Can Waste Valuable Individual	
	Information	29
	How Effective Can QRA Be?	31
	Summary and Conclusions	32
2	Introduction to Engineering Risk Analysis	35
	Overview of Risk Analysis for Engineered Systems	35
	Example: Unreliable Communication with Reliable Components	37

	Example: Optimal Number of Redundant Components	37
	Example: Optimal Scheduling of Risky Inspections	38
	Using Risk Analysis to Improve Decisions	39
	Hazard Identification: What Should We Worry About?	39
	Example: Fault Tree Calculations for Car Accidents	
	at an Intersection	40
	Structuring Risk Quantification and Displaying Results: Models	
	for Accident Probabilities and Consequences	41
	Example: Bug-Counting Models of Software Reliability	42
	Example: Bug Counting models of Boltware tendening models	
	and Reservoirs	43
	Example: Different Individual Risks for the Same Exceedance	т.)
	Probability Curve	43
	Quantifying Model Components and Inputs	
	Modeling Interdemendent Inputs and Events	45
	Example: Analysis of Accident Precursors	75 76
	Example: Analysis of Accident Fleculsons	40
	Some Alternatives to Subjective Driver Distributions	41
	Some Alternatives to Subjective Prior Distributions	47
	Example: Effects of Exposure to Contaminated Soft	49
	Example: The Rule of Three for Negative Evidence	54
	Example: A Sharp Transition in a Symmetric Multistage	<i></i>
	Model of Carcinogenesis	55
	Dealing with Model Uncertainty: Bayesian Model Averaging (BMA)	50
	and Alternatives	50
	Risk Characterization	58
	Engineering vs. Financial Characterizations of "Risk": Why Risk	50
		38
	Incompatibility of Two Suggested Principles for Financial	<i>(</i> )
	Risk Analysis	62
	Challenges in Communicating the Results of PRAs	66
	Methods for Risk Management Decision Making	67
	Example: A Bounded-Regret Strategy for Replacing	
	Unreliable Equipment	68
	Methods of Risk Management to Avoid	69
	Game-Theory Models for Risk Management Decision Making	70
	Game-Theory Models for Security and Infrastructure Protection	70
	Game-Theory Models of Risk-Informed Regulation	71
	Conclusions	72
-		
3	Introduction to Health Risk Analysis	73
	Introduction	73
	Quantitative Definition of Health Risk	75
	Example: Statistical and Causal Risk Relations May Have	
	Opposite Signs	76
	A Bayesian Network Framework for Health Risk Assessment	17
+		

c

Hazard Identification	80
Example: Some Traditional Criteria for Causality Fail to Refute	
Other Explanations	83
Exposure Assessment	85
Example: Simulation of Exposures to Pathogens in Chicken Meat	87
Example: Mixture Distributions and Unknown Dose-Response	
Models	88
Dose-Response Modeling	89
Example: Apparent Thresholds in Cancer Dose-Response Data	90
Example: Best-Fitting Parametric Models May Not Fit Adequately	91
Risk and Uncertainty Characterization for Risk Management	93
Example: Risk Characterization Outputs	93
Conclusions	96

#### Part II Avoiding Bad Risk Analysis

4	Limitations of Risk Assessment Using Risk Matrices
	Introductory Concepts and Examples
	A Normative Decision-Analytic Framework
	Logical Compatibility of Risk Matrices with Quantitative Risks 108
	Definition of Weak Consistency 109
	Discussion of Weak Consistency 109
	Logical Implications of Weak Consistency
	The Betweenness Axiom: Motivation and Implications
	Consistent Coloring 112
	Implications of the Three Axioms 113
	Example: The Two Possible Colorings of a Standard
	5 × 5 Risk Matrix
	Risk Matrices with Too Many Colors Give Spurious Resolution 114
	Example: A 4 × 4 Matrix for Project Risk Analysis
	Risk Ratings Do Not Necessarily Support Good Resource Allocation
	Decisions 117
	Example: Priorities Based on Risk Matrices Violate
	Translation Invariance
	Example: Priority Ranking Does Not Necessarily Support
	Good Decisions
	Categorization of Uncertain Consequences Is Inherently Subjective 119
	Example: Severity Ratings Depend on Subjective Risk Attitudes 119
	Example: Pragmatic Limitations of Guidance from Standards 120
	Example: Inappropriate Risk Ratings in Enterprise Risk
	Management (ERM) 121
	Discussion and Conclusions 122
	Appendix A: A Proof of Theorem 1 123

5	Limitations of Quantitative Risk Assessment Using Aggregate
	Exposure and Risk Models
	What Is Frequency?
	An Example: Comparing Two Risks 127
	Event Frequencies in Renewal Processes
	Example: Average Annual Frequency for Exponentially Distributed
	Lifetimes
	The "Frequency" Concept for Nonexponential Failure Times 128
	Example: Average Annual Frequency for Uniformly
	Distributed Lifetimes
	Conflicts Among Different Criteria for Comparing Failure
	Time Distributions
	Do These Distinctions Really Matter?
	Summary of Limitations of the "Frequency" Concept
	Limitations of Aggregate Exposure Metrics 133
	Use of Aggregate Exposure Metrics in Risk Assessment
	Aggregate Exposure Information May Not Support
	Improved Decisions
	Example: How Aggregate Exposure Information Can Be Worse
	Than Useless
	Multicollinearity and Aggregate Exposure Data
	Example: Multicollinearity Can Prevent Effective Extrapolation
	of Risk
	A Practical Example: Different Predictions of Asbestos Risks
	at El Dorado Hills, CA
	Summary of Limitations of Risk Assessments Based on Aggregate
	Exposure Metrics
	Limitations of Aggregate Exposure-Response Models: An Antimicrobial
	Risk Assessment Case Study 141
	Statistical vs. Causal Relations
	Example: Significant Positive K for Statistically Independent
	Risk and Exposure
	Example: A Positive K Does Not Imply That Risk Increases
	with Exposure
	Example: Statistical Relations Do Not Predict Effects of Changes 143
	Prevalence vs. Microbial Load as Exposure Metrics
	Attribution vs. Causation
	Human Harm from Resistant vs. Susceptible Illnesses
	Summary of Limitations of Aggregate Exposure-Response Model,
	$Risk = K \times Exposure \dots 148$
	Some Limitations of Risk Priority-Scoring Methods
	Motivating Examples
	Example: Scoring Information Technology Vulnerabilities
	Example: Scoring Consumer Credit Risks
	Example: Scoring Superfund Sites to Determine Funding Priorities 151

r

-

.

Example: Priority Scoring of Bioterrorism Agents	51
Example: Threat-Vulnerability-Consequence (TVC) Risk Scores	
and Risk Matrices	52
Priorities for Known Risk Reductions	52
Priorities for Independent, Normally Distributed Risk Reductions 15	53
Priority Ratings Yield Poor Risk Management Strategies	
for Correlated Risks	55
Example: Priority Rules Overlook Opportunities	
for Risk-Free Gains	55
Example: Priority Setting Can Recommend the Worst	
Possible Resource Allocation	6
Example: Priority Setting Ignores Opportunities for Coordinated	
Defenses	57
Priority Rules Ignore Aversion to Large-Scale Uncertainties	58
Discussion and Conclusions on Risk Priority-Scoring Systems 15	;9
Conclusions	50

### Part III Principles for Doing Better

6	Identifying Nonlinear Causal Relations in Large Data Sets
	Nonlinear Exposure-Response Relations 166
	Entropy, Mutual Information, and Conditional Independence
	Classification Trees and Causal Graphs via Information Theory 170
	Illustration for the Campylobacteriosis Case Control Data 173
	Conclusions
7	Overcoming Preconceptions and Confirmation Biases Using Data
	Mining
	Confirmation Bias in Causal Inferences
	Example: The Wason Selection Task
	Example: Attributing Antibiotic Resistance to Specific Causes
	Study Design: Hospitalization Might Explain Observed
	Resistance Data
	Choice of Endpoints
	Ouantitative Statistical Methods and Analysis
	Results of Ouantitative Risk Assessment Modeling for vatE
	Resistance Determinant
	Results for Inducible Resistance
	Discussion and Implications for Previous Conclusions
	Summary and Conclusions
	Appendix A: Computing Adjusted Ratios of Medians
	and their Confidence Limits 201

8	Estimating the Fraction of Disease Caused by One Component
~	of a Complex Mixture: Bounds for Lung Cancer
	Motivation: Estimating Fractions of Illnesses Preventable by Removing
	Specific Exposures
	Why Not Use Population Attributable Fractions?
	Example: Attribution of Risk to Consequences Instead of Causes 204
	Example: Positive Attributable Risk is Compatible with Negative
	Causation
	Theory: Paths, Event Probabilities, Bounds on Causation
	A Bayesian Motivation for the Attributable Fraction Formula
	The Smoking-PAH-BPDE-p53-Lung Cancer Causal Pathway
	Applying the Theory: Quantifying the Contribution
	of the Smoking-PAH-BPDE-p53 Pathway to Lung Cancer Risk 212
	A Simple Theoretical Calculation Using Causal Fractions
	Step 1: Replace Causal Fractions with Fractions Based
	on Occurrence Rates
	Step 2: Quantify Occurrence Rates Using Molecular-Level Data 216
	Step 3: Combine Upper-Bound Surrogate Fractions
	for Events in a Path Set 218
	Uncertainties and Sensitivities
	Discussion
	Conclusions
9	Bounding Resistance Risks for Penicillin
	Background, Hazard Identification and Scope: Reducing
	Ampicillin-Resistant E. faecium (AREF) Infections in ICU Patients 223
	Methods and Data: Upper Bounds for Preventable Mortalities
	Estimated Number of ICU Infections per Year
	Fraction of ICU Infections Caused by E. faecium
	Fraction of ICU E. faecium Infections That Are Ampicillin-Resistant
	and Exogenous (Nonnosocomial)
	Fraction of Vancomycin-Susceptible Cases
	Fraction of Exogenous Cases Potentially from Food Animals 229
	Penicillin Allergies
	Excess Mortalities 231
	Results Summary, Sensitivity, and Uncertainty Analysis
	Summary and Conclusions
10	Confronting Uncertain Causal Mechanisms – Portfolios
	of Possibilities
	Background: Cadmium and Smoking Risk
	Previous Cadmium-Lung Cancer Risk Studies
	Cadmium Compounds are Rat Lung Carcinogens
	Epidemiological Data are Inconclusive

f

	Pharmacokinetic Data Show That Smoking Increases Cadmium	
	Levels in the Human Lung	240
	Biological Mechanisms of Cadmium Lung Carcinogenesis	242
	A Transition Model Simplifies the Description	
	of Cadmium-Induced Lung Carcinogenesis	242
	Cadmium Can Affect Lung Carcinogenesis via	
	Multiple Mechanisms	244
	Smoking and Cd Exposures Stimulate Reactive Oxygen Species	
	(ROS) Production	245
	Cadmium Inhibits DNA Repair and Is a Co-Carcinogen for PAHs	248
	Quantifying Potential Cadmium Effects on Lung Cancer Risk	251
	Polymorphism Evidence on Lung Cancer Risks from Different	
	Mechanisms	252
	Quasi-Steady-State Analysis	252
	A Portfolio Approach to Estimating the Preventable Fraction	
	of Risk for Cd	256
	Discussion and Conclusions	257
	Appendix A: Relative Risk Framework	258
11	Determining What Can Be Predicted: Identifiability	261
	Identifiability	262
	Example 1: A Simple Example of Nonidentifiability	262
	Example 2: Unique Identifiability in a Two-Stage Clonal	
	Expansion Model	262
	Multistage Clonal Expansion (MSCE) Models of Carcinogenesis	266
	Nonunique Identifiability of Multistage Models	
	from Input-Output Data	270
	Example 3: Counting $5 \times 5$ Matrices with Sign Restrictions	270
	Example 4: Two Equally Likely Effects of Reducing	
	a Transition Rate	271
	Discussion and Conclusions	275
	Appendix A: Proof of Theorem 1	277
	Appendix B: Listing of ITHINK <sup>TM</sup> Model Equations for the Example	
	in Figure 11.3	279

#### Part IV Applications and Extensions

12	Predicting the Effects of Changes: Could Removing Arsenic
	from Tobacco Smoke Significantly Reduce Smoker Risks
	of Lung Cancer?
	Biologically Based Risk Assessment Modeling
	Arsenic as a Potential Human Lung Carcinogen
	Data, Methods, and Models

	A Multistage Clonal Expansion (MSCE) Framework for Lung Field Cancerization
13	Simplifying Complex Dynamic Networks: A Model of Protease Imbalance and COPD Dynamic Dose-Response
	Background on COPD
	A Flow Process Network Model of Protease-Antiprotease
	Imbalance in COPD 305
	Mathematical Analysis of the Protease-Antiprotease Network
	Some Possible Implications for Experimental and Clinical COPD 313
	Is the Model Consistent with Available Human Data?
	Summary and Conclusions 316
	Appendix A: Equilibrium in Networks of Homeostatic Processes 317
	Representing Biological Knowledge by Networks of Flow Processes317 Example: ODE and ITHINK <sup>®</sup> Representations
	of a Single Process
	Reducing Chains of Coupled Processes to Simpler Equivalents 320
14	Value of Information (VOI) in Risk Management Policies for Tracking and Testing Imported Cattle for BSE
	Testing Canadian Cattle for Bovine Spongiform Encephalitis (BSE) 327
	Methods and Data
	Formulation of the Risk Management Decision Problem
	as a Decision Tree
	Estimated Economic Consequences of Detecting Additional
	BSE Cases
	Scenario Probabilities
	Solution Algorithms
	Results
	Optimal Decision Rule for the Base Case
	Sensitivity Analysis Results
	Discussion
	Epilogue and Conclusions
	Appendix: Market Impact Assumptions and Calculations

. f

15	Improving Antiterrorism Risk Analysis	. 351
	The $Risk = Threat \times Vulnerability \times Consequence$ Framework	. 351
	RAMCAP <sup>TM</sup> Qualitative Risk Assessment	. 353
	Limitations of RAMCAP <sup>TM</sup> for Quantitative Risk Assessment	. 354
	Example: Distortions Due to Use of Arithmetic Averages	
	on Logarithmic Scales	. 355
	Example: Limited Resolution	. 355
	Example: Manipulating Vulnerability Estimates by Aggregating	
	Attack Scenarios	. 355
	Example: Nonadditive Vulnerabilities	. 356
	Example: Product of Expected Values Not Equal to Expected	
	Value of Product	. 356
	Risk Rankings Are Not Adequate for Resource Allocation	. 357
	Example: Priority Ranking May Not Support Effective Resource	
	Allocation	. 358
	Some Fundamental Limitations of $Risk = Threat \times$	
	Vulnerability × Consequence	. 358
	"Threat" Is Not Necessarily Well Defined	. 359
	"Vulnerability" Can Be Ambiguous and Difficult to Calculate	
	via Event Trees	. 360
	"Consequence" Can Be Ambiguous and/or Subjective	. 367
	Discussion and Conclusions	. 367
16	Designing Resilient Telecommunications Networks	. 371
16	<b>Designing Resilient Telecommunications Networks</b> Introduction: Designing Telecommunications Infrastructure Networks	. 371
16	<b>Designing Resilient Telecommunications Networks</b> Introduction: Designing Telecommunications Infrastructure Networks to Survive Intelligent Attacks	. 371 . 372
16	<b>Designing Resilient Telecommunications Networks</b> Introduction: Designing Telecommunications Infrastructure Networks to Survive Intelligent Attacks Background: Diverse Routing, Protection Paths, and Protection	. 371 . 372
16	Designing Resilient Telecommunications Networks Introduction: Designing Telecommunications Infrastructure Networks to Survive Intelligent Attacks Background: Diverse Routing, Protection Paths, and Protection Switching	. 371 . 372 . 372
16	Designing Resilient Telecommunications NetworksIntroduction: Designing Telecommunications Infrastructure Networksto Survive Intelligent AttacksBackground: Diverse Routing, Protection Paths, and ProtectionSwitchingAutomated Protection Switching (APS) for Packets and Light Paths	. 371 . 372 . 372 . 373
16	Designing Resilient Telecommunications Networks   Introduction: Designing Telecommunications Infrastructure Networks   to Survive Intelligent Attacks   Background: Diverse Routing, Protection Paths, and Protection   Switching   Automated Protection Switching (APS) for Packets and Light Paths   Demands Consist of Origins, Destinations, and Bandwidth	. 371 . 372 . 372 . 373
16	Designing Resilient Telecommunications Networks   Introduction: Designing Telecommunications Infrastructure Networks   to Survive Intelligent Attacks   Background: Diverse Routing, Protection Paths, and Protection   Switching   Automated Protection Switching (APS) for Packets and Light Paths   Demands Consist of Origins, Destinations, and Bandwidth   Requirements	. 371 . 372 . 372 . 373 . 373
16	Designing Resilient Telecommunications Networks   Introduction: Designing Telecommunications Infrastructure Networks   to Survive Intelligent Attacks   Background: Diverse Routing, Protection Paths, and Protection   Switching   Automated Protection Switching (APS) for Packets and Light Paths   Demands Consist of Origins, Destinations, and Bandwidth   Requirements   Multiple Levels of Protection for Demands	. 371 . 372 . 372 . 373 . 373 . 373
16	Designing Resilient Telecommunications Networks   Introduction: Designing Telecommunications Infrastructure Networks   to Survive Intelligent Attacks   Background: Diverse Routing, Protection Paths, and Protection   Switching   Automated Protection Switching (APS) for Packets and Light Paths   Demands Consist of Origins, Destinations, and Bandwidth   Requirements   Multiple Levels of Protection for Demands   A Simple Two-Stage Attacker-Defender Model	. 371 . 372 . 372 . 373 . 373 . 374 . 376
16	Designing Resilient Telecommunications Networks   Introduction: Designing Telecommunications Infrastructure Networks   to Survive Intelligent Attacks   Background: Diverse Routing, Protection Paths, and Protection   Switching   Automated Protection Switching (APS) for Packets and Light Paths   Demands Consist of Origins, Destinations, and Bandwidth   Requirements   Multiple Levels of Protection for Demands   A Simple Two-Stage Attacker-Defender Model   Results for Networks with Dedicated Routes ("Circuit-Switched"	. 371 . 372 . 372 . 373 . 373 . 374 . 376
16	Designing Resilient Telecommunications Networks   Introduction: Designing Telecommunications Infrastructure Networks   to Survive Intelligent Attacks   Background: Diverse Routing, Protection Paths, and Protection   Switching   Automated Protection Switching (APS) for Packets and Light Paths   Demands Consist of Origins, Destinations, and Bandwidth   Requirements   Multiple Levels of Protection for Demands   A Simple Two-Stage Attacker-Defender Model   Results for Networks with Dedicated Routes ("Circuit-Switched"   Networks)	. 371 . 372 . 372 . 373 . 373 . 373 . 374 . 376 . 377
16	Designing Resilient Telecommunications Networks   Introduction: Designing Telecommunications Infrastructure Networks   to Survive Intelligent Attacks   Background: Diverse Routing, Protection Paths, and Protection   Switching   Automated Protection Switching (APS) for Packets and Light Paths   Demands Consist of Origins, Destinations, and Bandwidth   Requirements   Multiple Levels of Protection for Demands   A Simple Two-Stage Attacker-Defender Model   Results for Networks with Dedicated Routes ("Circuit-Switched"   Networks)   Designing Networks to Withstand a Single (k = 1) Link Cut	. 371 . 372 . 372 . 373 . 373 . 373 . 374 . 376 . 377 . 377
16	Designing Resilient Telecommunications Networks   Introduction: Designing Telecommunications Infrastructure Networks   to Survive Intelligent Attacks   Background: Diverse Routing, Protection Paths, and Protection   Switching   Automated Protection Switching (APS) for Packets and Light Paths   Demands Consist of Origins, Destinations, and Bandwidth   Requirements   Multiple Levels of Protection for Demands   A Simple Two-Stage Attacker-Defender Model   Results for Networks with Dedicated Routes ("Circuit-Switched"   Networks)   Designing Networks to Withstand a Single (k = 1) Link Cut   Designing Networks to Withstand k = 2 Link Cuts	. 371 . 372 . 372 . 373 . 373 . 373 . 374 . 376 . 377 . 377 . 380
16	Designing Resilient Telecommunications Networks   Introduction: Designing Telecommunications Infrastructure Networks   to Survive Intelligent Attacks   Background: Diverse Routing, Protection Paths, and Protection   Switching   Automated Protection Switching (APS) for Packets and Light Paths   Demands Consist of Origins, Destinations, and Bandwidth   Requirements   Multiple Levels of Protection for Demands   A Simple Two-Stage Attacker-Defender Model   Results for Networks with Dedicated Routes ("Circuit-Switched"   Networks)   Designing Networks to Withstand a Single (k = 1) Link Cut   Designing Networks to Withstand k = 2 Link Cuts   Results for the General Case of k Cuts	. 371 . 372 . 372 . 373 . 373 . 373 . 374 . 376 . 377 . 380 . 380
16	Designing Resilient Telecommunications Networks   Introduction: Designing Telecommunications Infrastructure Networks   to Survive Intelligent Attacks   Background: Diverse Routing, Protection Paths, and Protection   Switching   Automated Protection Switching (APS) for Packets and Light Paths   Demands Consist of Origins, Destinations, and Bandwidth   Requirements   Multiple Levels of Protection for Demands   A Simple Two-Stage Attacker-Defender Model   Results for Networks with Dedicated Routes ("Circuit-Switched"   Networks)   Designing Networks to Withstand a Single (k = 1) Link Cut   Designing Networks to Withstand k = 2 Link Cuts   Results for the General Case of k Cuts   Statistical Risk Models and Results for Scale-Free Packet Networks	. 371 . 372 . 372 . 373 . 373 . 373 . 374 . 376 . 377 . 377 . 380 . 380 . 381
16	Designing Resilient Telecommunications Networks   Introduction: Designing Telecommunications Infrastructure Networks   to Survive Intelligent Attacks   Background: Diverse Routing, Protection Paths, and Protection   Switching   Automated Protection Switching (APS) for Packets and Light Paths   Demands Consist of Origins, Destinations, and Bandwidth   Requirements   Multiple Levels of Protection for Demands   A Simple Two-Stage Attacker-Defender Model   Results for Networks with Dedicated Routes ("Circuit-Switched"   Networks)   Designing Networks to Withstand a Single (k = 1) Link Cut   Designing Networks to Withstand k = 2 Link Cuts   Results for the General Case of k Cuts   Statistical Risk Models and Results for Scale-Free Packet Networks   Real-World Implementation Challenges: Incentives to Invest	. 371 . 372 . 372 . 373 . 373 . 373 . 374 . 376 . 377 . 377 . 380 . 380 . 381
16	Designing Resilient Telecommunications Networks   Introduction: Designing Telecommunications Infrastructure Networks   to Survive Intelligent Attacks   Background: Diverse Routing, Protection Paths, and Protection   Switching   Automated Protection Switching (APS) for Packets and Light Paths   Demands Consist of Origins, Destinations, and Bandwidth   Requirements   Multiple Levels of Protection for Demands   A Simple Two-Stage Attacker-Defender Model   Results for Networks with Dedicated Routes ("Circuit-Switched"   Networks)   Designing Networks to Withstand a Single (k = 1) Link Cut   Designing Networks to Withstand k = 2 Link Cuts   Results for the General Case of k Cuts   Statistical Risk Models and Results for Scale-Free Packet Networks   Real-World Implementation Challenges: Incentives to Invest in Protection	. 371 . 372 . 372 . 373 . 373 . 373 . 374 . 376 . 377 . 380 . 381 . 384
16	Designing Resilient Telecommunications Networks   Introduction: Designing Telecommunications Infrastructure Networks   to Survive Intelligent Attacks   Background: Diverse Routing, Protection Paths, and Protection   Switching   Automated Protection Switching (APS) for Packets and Light Paths   Demands Consist of Origins, Destinations, and Bandwidth   Requirements   Multiple Levels of Protection for Demands   A Simple Two-Stage Attacker-Defender Model   Results for Networks with Dedicated Routes ("Circuit-Switched"   Networks)   Designing Networks to Withstand a Single (k = 1) Link Cut   Designing Networks to Withstand k = 2 Link Cuts   Results for the General Case of k Cuts   Statistical Risk Models and Results for Scale-Free Packet Networks   Real-World Implementation Challenges: Incentives to Invest   in Protection   Example: An N-Person Prisoner's Dilemma for Network	. 371 . 372 . 372 . 373 . 373 . 374 . 376 . 377 . 377 . 380 . 381 . 384
16	Designing Resilient Telecommunications NetworksIntroduction: Designing Telecommunications Infrastructure Networksto Survive Intelligent AttacksBackground: Diverse Routing, Protection Paths, and ProtectionSwitchingAutomated Protection Switching (APS) for Packets and Light PathsDemands Consist of Origins, Destinations, and BandwidthRequirementsMultiple Levels of Protection for DemandsA Simple Two-Stage Attacker-Defender ModelResults for Networks with Dedicated Routes ("Circuit-Switched"Networks)Designing Networks to Withstand a Single (k = 1) Link CutDesigning Networks to Withstand k = 2 Link CutsResults for the General Case of k CutsStatistical Risk Models and Results for Scale-Free Packet NetworksReal-World Implementation Challenges: Incentives to Investin ProtectionExample: An N-Person Prisoner's Dilemma for NetworkMaintenance	. 371 . 372 . 372 . 373 . 373 . 373 . 374 . 376 . 377 . 380 . 380 . 381 . 384 . 385
16	Designing Resilient Telecommunications Networks   Introduction: Designing Telecommunications Infrastructure Networks   to Survive Intelligent Attacks   Background: Diverse Routing, Protection Paths, and Protection   Switching   Automated Protection Switching (APS) for Packets and Light Paths   Demands Consist of Origins, Destinations, and Bandwidth   Requirements   Multiple Levels of Protection for Demands   A Simple Two-Stage Attacker-Defender Model   Results for Networks with Dedicated Routes ("Circuit-Switched"   Networks)   Designing Networks to Withstand a Single (k = 1) Link Cut   Designing Networks to Withstand k = 2 Link Cuts   Results for the General Case of k Cuts   Statistical Risk Models and Results for Scale-Free Packet Networks   Real-World Implementation Challenges: Incentives to Invest   in Protection   Example: An N-Person Prisoner's Dilemma for Network   Maintenance   Example: Nash Equilibrium Can Be Inadequate for Predicting	. 371 . 372 . 372 . 373 . 373 . 373 . 374 . 376 . 377 . 377 . 377 . 380 . 381 . 384 . 385

Example: A Network Collusion Game with an Empty Core	387
Example: A Tipping Point	388
Summary	388
Epilogue	389
References	391
Index	423

•