

Contents

ABOUT THE AUTHORS	xv
FOREWORD	xvii
PREFACE	xix
ACKNOWLEDGMENTS	xxiii

Part I Introduction

CHAPTER 1 Introduction to Science	3
<i>Mark Tardiff</i>	
Chapter Objectives	4
What Is Science	4
Types of Science	5
Science Is Messy	6
Hierarchy of Evidence	9
From Ptolemy to Einstein—Science and the Discovery of the Nature of the Sky	10
A Science Continuum of Discovery	11
The Ptolemaic Model and Supporting Assumptions	13
Was the Ptolemaic Model of the Solar System Useful?	16
Emergence of the Heliocentric Model	16
Nicolaus Copernicus	17
Was the Copernican Model an Improvement?	19
Johannes Kepler	19
Kepler's Contributions in the Context of the Science Continuum of Discovery	21
Galileo Galilei	21
Galileo's Contributions in the Context of the Science Continuum of Discovery	23
Isaac Newton	23
Newton's Contributions in the Context of the Science Continuum of Discovery	25
Albert Einstein	26
Are Einstein's Contributions an Improvement to Understanding Planetary Motion?	27

Einstein's Contributions in the Context of the Science	
Continuum of Discovery.....	28
Summary and Conclusions.....	29
Discovery in the Realm of Right and Wrong.....	30
Endnotes.....	31

CHAPTER 2	Science and Cyber Security	33
	Chapter Objectives.....	34
	Defining Cyber Space	34
	Data Perspective	34
	Technology Perspective	35
	Cybernetic Perspective	35
	Defining Cyber Security.....	36
	Attributes of Cyber Security	37
	Cyber Security Fundamentals	39
	Vulnerability.....	39
	Exploit.....	39
	Threat.....	40
	Threat Actor.....	40
	Threat Vector	40
	Attack	40
	Malware	40
	Secure System Design Principles.....	41
	Cyber Security Controls Overview.....	43
	Access Control	44
	Situation Awareness	45
	Cryptography	46
	Host Security	49
	Network Security.....	50
	Risk.....	50
	Defining a Science of Cyber Security.....	51
	Our Definition of a Cyber Security Science	52
	Challenges in Achieving Security in Cyber Space.....	55
	Further Reading.....	57
	Attack Detection	57
	Secure Mechanism Design.....	57
	Software Security	57
	Malware/Threat Analysis.....	57
	Risk Management	58
	Cryptography	58
	Endnotes.....	61

CHAPTER 3	Starting Your Research	63
	Chapter Objectives.....	65
	Starting Your Research	65

Initial Question Process	67
Research Progression	68
Observational Research	70
Theoretical Research	71
Experimental Research	73
Applied Research	74
Research Before the Research	75
Selecting Your Research Path	78
Walking the Decision Tree	79
Observation Method Selection	84
Theoretical Method Selection	86
Experimental Method Selection	87
Applied Method Selection	89
Conferences and Journals	90
Endnotes	91

Part II Observational Research Methods

CHAPTER 4 Exploratory Study	95
Chapter Objectives	96
Knowledge by Inference	96
Types of Studies	98
Exploratory Study	98
Gathering Data	100
Research Questions and Datasets	102
Scales of Data	103
Sample Size	104
Dataset Sensitivities and Restrictions	109
Exploratory Method Selection	109
Exploratory Study Method Examples	111
Case-control Example	112
Ecological Example	114
Cross-sectional	116
Longitudinal Example	118
Analysis Bias	121
The Search for a Causal Relationship	123
Graph Summarization	123
Descriptive Statistics	123
Regression Analysis	124
Reporting Your Results	126
Sample Format	127
Endnotes	129
 CHAPTER 5 Descriptive Study	131
Chapter Objectives	132
Descriptive Study Methods	132

Observation Method Selection	135
Gathering Data	135
Data Collection Methods	137
Data Analysis	140
Coding Unstructured Data	141
Proportions	141
Frequency Statistics	142
Descriptive Study Method Examples	142
Case Study	143
Elicitation Studies	145
Case Report	147
Reporting Your Results	148
Sample Format	148
Endnotes	151
 CHAPTER 6 Machine Learning	153
<i>Satish Chikkagoudar, Samrat Chatterjee,</i>	
<i>Dennis G. Thomas, Thomas E. Carroll, and George Muller</i>	
Chapter Objectives	153
What is Machine Learning	154
Categories of Machine Learning	154
Debugging Machine Learning	157
Bayesian Network Mathematical Preliminaries and Model	
Properties	158
Strengths and Limitations	158
Data-driven Learning and Probabilistic Inference	
within Bayesian Networks	159
Parameter Learning	159
Probabilistic Inference	160
Notional Example with bnlearn Package in R	160
Hidden Markov Models	165
Notional Example with HMM Package in R	167
Discussion	169
Sample Format	169
Abstract	169
Introduction	170
Related Work	170
Approach	170
Evaluation	170
Data Analysis/Results	171
Discussion/Future Work	171
Conclusion/Summary	171
Acknowledgments	171
References	171
Endnotes	172

Part III Mathematical Research Methods

CHAPTER 7	Theoretical Research	177
	<i>Thomas E. Carroll</i>	
	Chapter Objectives.....	177
	Background	177
	Characteristics of a Good Theory	179
	Challenges in Development of Cyber Security Science Theory	180
	Identify Insight	181
	Determine Relevant Factors	182
	Formally Define Theory	182
	Test for Internal Consistency	183
	Test for External Consistency	183
	Refute	184
	Continue to Seek Refinements.....	184
	Example Theoretical Research Construction.....	184
	Reporting Your Results	188
	Sample Format.....	188
	Endnotes.....	191
 CHAPTER 8	 Using Simulation for Research.....	 193
	Chapter Objectives.....	194
	Defining Simulation	194
	When Should Simulation Be Used	196
	Theoretical Simulations	196
	Simulation for Decision Support.....	197
	Empirical Simulation	197
	Synthetic Conditions.....	198
	Cautions of Simulation Use	199
	Defining What to Model.....	199
	Model Validity	201
	Instantiating a Model.....	202
	Types of Simulation.....	203
	Example Use Case.....	207
	Paper Format.....	210
	Endnotes.....	210

Part IV Experimental Research Methods

CHAPTER 9	Hypothetico-deductive Research	215
	Chapter Objectives.....	215
	Purpose of Hypothesis-Driven Experimentation	215

Turn Inductive Process Into Deductive Process	216
Reject a Theory or Build Evidence Strengthening.....	217
Specify What You Think is Involved; Challenge Assumptions	217
Define a Process by Which Others can Replicate and Reproduce the Effect; to Test and Ensure that Your Own Approach is Valid.	218
The Goal of Hypothetico-deductive Experimentation is Different than Applied Experimentation	218
A Proper Hypothesis.....	219
Observable and Testable	219
Clearly Defined	220
Single Concept.....	221
Predictive	222
Generating a Hypothesis from a Theory.....	222
Experimentation.....	224
Dependent Variables (Measured Variables)	226
Independent Variables (Controls)	228
Experimental Design.....	232
Analysis.....	239
Hypothesis Testing	239
Integrating the Theory with Results.....	244
Reporting Your Results	245
Sample Format.....	245
Endnotes.....	248
CHAPTER 10 Quasi-experimental Research	251
Chapter Objectives.....	252
True versus Quasi-experiment	252
Cyber Drivers for Quasi-experimental Design	253
Quasi-experiment Research Methods.....	255
Difference-of-differences Design	255
Time Series Design	260
Cohort Design	264
Reporting Your Results	268
Endnotes.....	268
Part V Applied Research Methods	
CHAPTER 11 Applied Experimentation	271
Chapter Objectives.....	272
Building From a Theory	272
Methods of Applied Experimentation	273
Benchmarking.....	274
Collecting or Defining a Benchmark	276
Running the Benchmark.....	279

Analyzing the Results	280
Problems With Benchmarking	283
Reporting Your Results	284
Sample Format	284
Validation Testing	287
Independent Variables	289
Dependent Variables	289
Experimental Design	290
Problems With Validation Testing	292
Reporting Your Results	293
Sample Format	294
Endnotes	297

CHAPTER 12 Applied Observational Study	299
Chapter Objectives	300
Applied Study Types	300
Applied Exploratory Studies	301
Applied Descriptive Study	304
Applied Observation Method Selection	306
Data Collection and Analysis	306
Applied Exploratory Studies	306
Applied Descriptive Studies	307
Applied Exploratory Study: Stress Test	307
System	308
Behavior	308
Testing Methodology	309
Applied Descriptive Study: Case Study	311
Reporting Your Results	313
Sample Format	314
Endnote	317

Part VI Additional Materials

CHAPTER 13 Instrumentation	321
Chapter Objectives	322
Understanding Your Data Needs	322
Fidelity	323
Types	326
Amount	326
Source location	327
Difference between Operational and Scientific Measurements	327
Overview of Data and Sensor Types	328
Host-based Sensors	328
Network-based Sensors	330

	Hardware Sensors	331
	Physical Sensors	332
	Honeypots	333
	Centralized Collectors	334
	Data Formats.....	334
	Sensor Calibration	337
	Controlled-Testing Environments	338
	Conclusion.....	342
	Endnotes.....	342
CHAPTER 14	Addressing the Adversary	345
	Chapter Objectives.....	346
	Defining Adversary.....	346
	The Challenge of Adversarial Research	348
	Adversaries in Other Fields of Study	353
	Different Ways to Think About Threats.....	356
	Adversary Perspective	357
	Defining Adversaries as Threats.....	358
	Attribution	359
	Integrating Adversary Models into Research	359
	Approaches	360
	Challenges	361
	Conclusions.....	365
	Endnotes.....	365
CHAPTER 15	Scientific Ethics	367
	Chapter Objectives.....	367
	Ethics for Science.....	367
	History of Ethics in Cyber Security.....	371
	Ethical Standards.....	374
	Association for Computing Machinery.....	374
	Institute of Electrical and Electronics Engineers.....	376
	IEEE Code of Ethics.....	376
	Ten Commandments of Computer Ethics.....	377
	Certification Bodies Ethics	378
	Cyber Security Expert Classification	378
	Cyber Security and the Law.....	379
	United States	379
	Canada	380
	United Kingdom.....	381
	France	381
	European Union.....	381
	Japan.....	381
	South Korea.....	382

Human Subjects Research.....	382
Institutional Review Board	383
Ethical Use of Data	384
Consent	385
Criminally Released Data	386
Individual Responsibility.....	387
Plagiarism.....	387
Authorship.....	388
Conclusion	389
Endnotes.....	389

INDEX 393

Steven J. Edgar is currently a Senior Cyber Security Specialist at the Pacific Northwest National Laboratory. He has completed research in the areas of secure communication protocols, cryptographic key management, critical infrastructure protection, and developing a lifecycle approach — cyber security. Edgar's research interests include the scientific underpinnings of cyber security and inspiring scientific-based cyber security solutions to enterprise and critical infrastructure environments. His expertise lies in scientific process, critical infrastructure security, protocol development, cyber forensics, network security, and tested and experiment construction. Edgar has a B.S. and M.S. in Computer Science from the University of Tulsa with a specialization in Information Research.

David D. Mann is currently a Senior Cyber Security Specialist in the National Security Directorate at the Pacific Northwest National Laboratory. He holds a B.S. in Computer and Information Science from the Robert D. Clark Honors College at the University of Oregon and a Ph.D. in Computer Science from the University of Idaho. Mann's work as a Ph.D. includes enterprise real-time and cyber security, secure control system communications, and critical infrastructure security. For his research is an application of advanced research methods for cyber security (Cyber Security Science). Prior to his position at PNNL, Mann spent 5 years as a researcher on Group Key Management Protocols for the Center for Secure and Dependable Systems at the University of Idaho (U of I). Mann also has experience in teaching undergraduate and graduate computer science courses at U of I, and as an adjunct faculty at Washington State University. Mann has co-authored numerous papers and presentations on cyber security, control system security, and cryptographic key management.