Contents

Foreword xxvii
Introduction xxix

Part I Understanding the Dark Side: Malicious Intent 1

Chapter 1 Analyzing the Malicious Individual 3
Analyzing the Unique Individual 4
Richard Reid: The Shoe Bomber 7
  The Event 7
  The Motivation 8
  Causes 9
  A Behavior Analysis 9
Ted Bundy: The Infamous Serial Murderer 11
  Similarities of Targets 12
  The Motivation 12
  Determining the Complexities Underlying Individual Malicious Behavior: A Behavior Analysis 13
  Removing Subjectivity and Bias from the Behavior Analysis 15
The Individual Cyber Attacker 15
  Identifying the Threat from the Lone Cyber Attacker 16
  Recognizing the Power of Being Anonymous 18
  Recognizing When a Hacker Is Detached from the Target 19
  Recognizing Motivation 20
  Identifying the Power of Disruption 21
  Recognizing the Need for Theft 23
  A Behavior Analysis 25
Modeling the Individual: Advantages and Disadvantages 25
  How Individuals May Vary 26
## Contents

- The Loner 27
- The Chameleon 27
- The Social Misfit 28
- The Individual versus the Group 29
- Advantages of AuBA #1: Automated Summarization 29
- In Summary 32

### Chapter 2  Analyzing the Malicious Group 35
- Understanding the Group Adversary 36
- Analyzing al-Qaeda 37
  - Automated Behavior Analysis Summary 37
  - The Organization 41
  - Group Dynamics 41
  - The Motivation 42
  - Declarations of War 42
  - A Behavior Analysis 43
- Analyzing Hezbollah 45
  - The Organization 45
  - Consistency of Behavior 46
  - The Motivation 47
  - Targeting Consistency 47
  - A Behavior Analysis 48
- Analyzing the Coordinated Group Cyber Threat 50
  - The Group Structure 53
  - The Motivation 56
  - A Behavior Analysis 57
- Advantages of AuBA #2: Theme-Guided Smart Searches 59
- In Summary 61

### Chapter 3  Analyzing Country-Level Threats 63
- Threats to Our National Infrastructure 64
- Analyzing the Specific Threat of Terrorist Attacks 69
  - Current Terrorist Threats to the United States 70
  - Preventing Terrorist Attacks on U.S. Soil 75
- Improving Network Security 78
  - Current Network Security 79
  - Current Foreign Threats to Network Security 82
  - Understanding Current Technology for Protecting Our Networks 83
- Facing Chemical, Biological, Radiological, and Nuclear (CBRN) Threats 84
  - Understanding the Threat of a Biological Attack 85
  - Anticipating the Dirty Bomb 86
- Advantages of AuBA #3: Reducing Errors and Inefficiencies of Manual Predictive Modeling 87
- In Summary 89
### Chapter 4 Threats and Security Nightmares: Our Current Reactive State of Security

- Analyzing Mall, School, Workplace, and Other Seemingly Random Public Violence...
- Making Sense of Seemingly Senseless Public Attacks...
- Why Are We Violent?
- Unanticipated Terrorist Network Attacks...
- Understanding the Element of Surprise...
- Anticipating the Unknown...
- Can Technology Detect First-Time Attacks?
- Detecting the New Attack...
- Advantages of AuBA #4: Building Predictive Applications...

### Chapter 5 Current Network Security

- Hacking and National Network Security...
- Growing Damage and Threat...
- Assessing Current Technology...
  - Signature Detection...
  - Forensics: The Key to Defining New Signatures for Detection...
  - False Negative: Missing the New Attack...
- Anomaly Detection...
  - Defining the Norm...
  - Unanticipated Network Attacks: The Bane of Network Security...
- Moving Toward Fixing Current Ineffective Network Protection...
- Winning or Losing?
- Adjusting Our Approach: The Need for a Paradigm Shift...
- Augmenting the Concept of Network Behavior with Human Behavior...
  - Identifying Human Intent by Analyzing Packets...
  - External Threat Assessment: CheckMate...
  - Internal Threat Assessment: InMate...
- Envisioning an Effective Future Network Protection Technology...
  - Enhancing Current Technology with Behavior Analysis...
  - Extracting Human Behavior from Digital Data...
- Advantages of AuBA #5: Conducting a Human Behavior Assessment of Threats from Network Packets...

### Chapter 6 Future Threats to Our National Security

- Our Growing National Security Dependency on Computers and Networks...
- Increasing Threat on a Global Basis...
The Ever-Increasing Sophistication of the Adversary 142
Anticipating Additional Asymmetric Warfare Attacks in the Future — Another 9/11? 145
Unanticipated Terrorist Attacks 146
Weapons of Mass Destruction 147
Water and Food Resources 148
Diminishing Effectiveness of Network Security 150
Decreasing Safety for Americans Worldwide Post Osama bin Laden 150
Threats to Our Fragile Financial Markets 152
The Dire Need for New Proactive Methods 154
Moving from Reactive to Proactive Methodology 155
Interjecting Behavior Analysis 155
Informed Security: Removing the Element of Surprise 155
Advantages of AuBA #6: Automated Pattern Classification 156
In Summary 158

Part II Dissecting Malicious Behavior 161
Chapter 7 Applying Behavior Principles: Predicting Individual Malicious Behavior 163
Using a Behavior Analysis Methodology That Works 163
Using Behavior Principles to Analyze Behavior 166
Environmental Variables 169
Different Environments, Different Antecedents 171
Antecedents, Behavior, and Consequences 172
Behavior Modeling 175
Automated Behavior Analysis (AuBA) 176
Using Tools to Assist Our Understanding 177
Predicting Adversarial Behavior 178
Influencing and Preventing Adversarial Behavior 178
Advantages of AuBA #7: Incorporating, Refining, and Expanding Behavior Principles for Global Security 180
In Summary 182

Chapter 8 Applying Behavior Principles: Predicting Group Malicious Behavior 183
Analyzing Threat 184
Group Attempts to Inflict Harm and Damage 185
When Threats Turn into Actions 185
Attempts to Steal and Deceive 187
Obtaining Data to Assist in Understanding Adversary Behavior 187
Moving from Applied Behavior Analysis and the Classroom to Global Adversary Behavior with AuBA 190
Determining Who, What, Where, When, and How from Historical Data 191
Chapter 11  Computer Networks: Protection from External Threat  
Protecting Against Known Attacks:
  Signature Detection 256
    Network Signature Detection 258
    Terrorism Signature Detection: A Comparison 259
    Identifying Criminal Signatures 260
  Identifying Unknown and First-Time Attacks 263
    Identifying Anomalies 266
      Network Anomaly Detection 267
      Advantages of Anomaly Detection 267
      Disadvantages of Anomaly Detection 267
      Methods of Detection 269
  Anticipating Anomalies 269
    Terrorism 270
    Networks 271
    Criminal Behavior 272
    Using Behavior Analysis to Identify
      New, First-Time Attacks 273
  Forensics: Studying and Defining the Past 273
    Is the Past the Best Predictor of Future Behavior? 274
    Updating How to Use Past Information 274
  Advantages of AuBA #11: Network Intrusion — Converting
    Digital Information to Human Behavior Assessment 275
In Summary 276

Chapter 12  Computer Networks: Protection from Internal Threat  
Defining the Insider 278
  The Significance of Insider Threat 279
  Discovering Malicious Intent: Insider Motivations 281
  Acting on Malicious Intent: Insider Behaviors 283
    Insider Methods of Operations 284
    Deception: The Primary Core of the Malicious Insider 290
    Behavior of an Insider Network Thief 291
  Current Trends in Insider Threat Protection 292
    A Lack of Proactive Capability 293
    Signature Detection and Rules 293
    Anomaly Detection: False Positives Waiting to Happen 293
Establishing the Need for a Paradigm Shift to Proactive Capabilities 294
The Top 10 Features of a Paradigm Shift in Network Security 294
AuBA, CheckMate, and InMate 295
Advantages of AuBA #12: Powerful Predictive Analysis Engines That Fit on a Laptop 296
In Summary 297

Chapter 13 Predicting Global Threat 299
Understanding State-Sponsored Threat 300
Organized State Support 301
Foreign State-Supported Terrorist Attacks 302
Foreign State-Supported Cyber Attacks 305
Describing and Identifying Future Global Threat 306
A Review of the AuBA Modeling Methods 311
AuBA Methodology 312
Automated Behavior Analysis Using Subject Matter Experts (AuBASME) 313
Understanding the Role of Network Forensics 317
Other Forensic Science Approaches Compared to Network Forensics 319
Using Past Events to Predict Future Events 319
Determining State Support of Terrorist Activities 321
Gathering Evidence of State-Supported Malicious Behavior 321
The Behaviorprint 322
From Fingerprints to Behaviorprints 324
Modeling as a Form of Proof 324
Moving from Detection to Protection: A Major Leap 325
Advantages of AuBA #13: The AuBA Behaviorprint and How It Compares to Signatures 326
In Summary 327

Part III Applying Tools and Methods 329
Chapter 14 Predictive Capability in Software: Tools for a New Approach 331
Fusing Computer and Behavioral Sciences 332
Sampling and Presidential Polls 333
High-Speed Automated Stock Market Prediction 334
AuBA Prediction of Terrorism 336
Using the Computer’s Speed and Memory to Our Benefit 337
Applying Simple Tools to Gain Advanced Results 338
Excel and the Analysis ToolPak: Methods and Examples 340
Advanced Tools: SPSS, SAS, and Other Statistical Packages 344
Human Bias: The Enemy to Accuracy and Analysis 345
An Example of Biased but Publishable Bad Research 346
Identifying Bias 349
Removing Bias via Automation 350
Automating Behavioral Principles: Applying AuBA 351
Capturing Cultural Nuances 352
Moving from Theory to Practice: A Necessary Transition 352
Advantages of AuBA #14: Incorporating Key Technological Advances 354
In Summary 355

Chapter 15  Predictive Behavioral Modeling: Automated Tools of the Trade 357
Automated Behavior Analysis (AuBA) 358
ThemeMate 359
   Human Interaction with AuBA Automated Features 361
   Language Independence 363
   Other ThemeMate Features, Including Cross-Language 364
Text Summarization: Automated CliffsNotes? 366
Identifying Predictive Indicators (Antecedents) 366
Constructing Data Arrays for Predictive Analysis 367
AutoAnalyzer 373
Using the Advantages of Speed, Accuracy, and Lack of Bias 375
   Speed 375
   Accuracy 375
   Bias 376
Conducting Behavioral Modeling: Integrating ThemeMate and AutoAnalyzer 377
In Summary 381

Chapter 16  Developing AuBA Applications 383
Modeling from Text Accounts of Past Behavior 384
   Modeling Adversaries and Adversarial Groups 386
   Extracting Significant Data from Past News Articles 387
   Testing Your Model 388
   Using Your Model to Predict 389
   Constructing Open Source Cyber Threat Models 390
Modeling from Sensor Output 393
   Predicting Malicious Behavior from Sensor Tracking of Movement 394
CheckMate and InMate: Implementing Behavior-Based Network Protection 396
   CheckMate Network Intrusion Protection System 397
   InMate Misuse Detection System 399
### Chapter 17 Mastering AuBA Tools for Real-World Use

Predicting the Unpredictable: Identifying Future Malicious Behavior
- Applying AuBA to Future Threat
- Current U.S. Citizen Trends to Aid Terrorism
  - Leaving the Country
  - Remaining Inside the United States as a Foreign Agent
  - Acting on Their Own
- Cyber Attacks
- Applying AuBA to Network Security
  - CheckMate: Protecting Networks from External Threat
  - InMate: Identifying Insider Threat
- Advantages of AuBA #17: Versatility

### Chapter 18 Analyzing Future Malicious Behavior

The Necessity of Context in Predicting Future Behavior
- Analyzing the Individual and the Group
  - Gathering Background Information
  - Selecting Documents for the Basic Corpus
  - Determining Inner Dynamics from External Data
  - Anticipating Adversarial Individual and Group Transition
  - What to Do When Data Is Missing
    - AuBASME: A New Method for Using Subject Matter Expertise
    - AuBASME and Prediction
- Analyzing Threat on a Global Level
  - Incorporating Multiple Models
  - Interpreting Results of Multiple Models
  - Anticipating Events
- Implications for Security
- Advantages of AuBA #18: Automated Characterization of Network Attacks

### Part IV Predicting Malicious Behavior: Tools and Methods to Support a Paradigm Shift in Security

### Chapter 19 AuBA Future Extensions Today

Predicting New Adversary Threat with Enhanced Accuracy
- Defining Future Signatures: The Department of Pre-crime?
- Converting Reactive Technology to Proactive Protection
Augmenting Signature Detection with AuBA 455
Augmenting Anomaly Detection with AuBA 456
The Elements of Proactive Security 458
A Behavioral Science–Based Paradigm Shift 459
Why We Need a New Approach to Security 463
Fall of the Soviet Union 463
September 11, 2001 (9/11) 464
Fall of Our Economic Foundation and the Bailout 464
Current Status 465
Advantages of AuBA #19: AuBA in the Future 469
In Summary 470

Chapter 20 How to Predict Malicious Behavior: A Walkthrough 471
A Manual Walkthrough of AuBA Principles 471
A Clinical Case Example 472
The Clinical Analysis and Solution 475
Further Clinical Examples 476
Moving Beyond the Clinical Setting to Expanded Environments: Automated Assist 479
Full Automation of the Prediction of Human Behavior: Automated Behavior Analysis 481
Walking Through the AuBA Methodology 485
Text as Input 486
Processing the Text Corpus of Your Choice with ThemeMate 488
Generating a Predictive Engine with AutoAnalyzer 491
Advantages of AuBA #20: Final Thoughts 494
In Summary 495

Appendix What’s on the DVD? 497
Index 501