## Contents

Part I  Counterterrorism History: Then and Now

1  September 11 Attacks  ..................................................  3
   1.1  September 11, 2001 .................................................  3
   1.2  Disney’s Responses to the 9/11 Attacks .........................  6
   1.3  FBI Warning of Hollywood as a Terrorist Target .............  7
   1.4  Hollywood Realism on Terrorism ...............................  8
   1.5  A New Day of Infamy and America at War ....................  9
   1.6  September 11, 2012 ............................................... 12
   1.7  Sony-pocalypse: Invoking 9/11 Attacks in Cyber Terrorism ... 12
   Bibliography .................................................................. 16

2  U.S. Intelligence Community ............................................. 21
   2.1  “Need to Know” — Truths, Half Truths, and Lies ............. 21
   2.2  FBI Ten Most Wanted Fugitive: Osama Bin Laden ........... 23
   2.3  An American Hero Born in Lebanon ........................... 25
   2.4  The FBI-CIA Bureaucratic Rivalries ........................... 26
   2.5  Operational Failures of the U.S. Intelligence Community ... 28
   2.6  Unity of Counterterrorism Effort Across U.S. Government ... 29
   2.7  Transition from Need-to-Know to Need-to-Share and Need-to-Provide ........................................... 31
   2.8  Informed Interrogation Approach ............................... 34
   2.9  U.S. Fusion Centers ................................................. 35
   2.10 International Collaboration on Counterterrorism .......... 36
   2.11 Hard Lessons from Pearl Harbor and 9/11 ................... 37
   Bibliography .................................................................. 39
Part II  Counterterrorism Strategies: Causes and Cures, War and Peace

3  Understanding Terrorism  ................................................................. 45
   3.1  “Give a Human Face to People We Consider Our Enemies” — The Americans  ......................................................... 46
   3.2  Bravery and Cowardice ................................................................. 48
   3.3  Drones Kill Terrorists, not Terrorism .................................................. 49
   3.4  War on Terror (Overseas Contingency Operation)  .............................. 52
   3.5  A Stubborn Terror ........................................................................ 53
   3.6  Economic and Psychological Warfare .................................................. 55
   3.7  Inside the Minds of Terrorists and Their Sympathizers  ......................... 58
   3.8  Questioning Terrorism and Destroying Stereotypes ......................... 62

Bibliography ................................................................. 64

4  Cures for Terrorism ........................................................................... 73
   4.1  Terrorism as a Disease .................................................................... 73
   4.2  “Revenge Is Sour” — George Orwell ................................................ 75
   4.3  “Govern Your Passions or They Will Be Your Undoing” — Mr. Spock ................................................................. 78
   4.4  “Impossible to Carry a Grudge and a Big Dream at the Same Time” — Unknown ................................................................. 79
   4.5  “Every Truth Has Two Sides” — Aesop ............................................. 80
   4.6  “Give Everyone a Voice” — Mark Zuckerberg .................................... 82
   4.7  “The Only Security of All Is in a Free Press” — Thomas Jefferson ............. 84
   4.8  “Free Speech Would not Protect a Man Falsely Shouting Fire” — Oliver Wendell Holmes, Jr ......................................................... 86
   4.9  “198 Methods of Nonviolent Action” — Gene Sharp ............................. 88
   4.10  “We Do not Have the Right to Resort to Violence When We Don’t Get Our Way” — President Bill Clinton  ............................. 96
   4.11  “Peace Is the Only Path to True Security” — President Barack Obama  ................................................................. 98

Bibliography ................................................................. 99

5  War and Peace ...................................................................................... 107
   5.1  War as State-Sponsored Terrorism .................................................... 108
   5.2  Complacency in War ....................................................................... 109
   5.3  The Warrior’s Code ....................................................................... 110
   5.4  Civilians Wanting Peace .................................................................... 111
   5.5  Peace Entailing Sacrifice ................................................................. 112
   5.6  Attainable Peace ............................................................................. 115
   5.7  A Just and Lasting Peace .................................................................. 117
   5.8  Peace and Friendships on Facebook .................................................. 119
### Part III Counterterrorism Technologies: Total Information Awareness

#### 6 The Rise and Fall of Total Information Awareness

6.1 President Ronald Reagan and Admiral John Poindexter .................................. 135  
6.2 Defense Advanced Research Projects Agency (DARPA) ......................... 136  
6.3 Information Awareness Office (IAO) ......................................................... 137  
6.4 Perception of Privacy Invasion ................................................................. 138  
6.5 Privacy Protection in Total Information Awareness (TIA) .......................... 139  
6.6 Opposing Views on TIA ........................................................................... 141  
6.7 Demystifying IAO and TIA ........................................................................ 143  
6.8 Demise of IAO and TIA .............................................................................. 145  
Bibliography ................................................................................................. 147

#### 7 The Afterlife of Total Information Awareness and Edward Snowden’s NSA Leaks

7.1 NSA’s Terrorist Surveillance Program ...................................................... 151  
7.2 President George W. Bush and NSA Warrantless Wiretapping ................ 153  
7.3 Poindexter’s Policy Analysis Market ......................................................... 155  
7.4 Project Argus: Bio-surveillance Priming System ...................................... 155  
7.5 President Barack Obama’s Big Data R&D Initiative ............................... 156  
7.6 Palantir Technologies Funded by CIA’s in-Q-Tel .................................... 157  
7.7 Microsoft and NYPD’s Domain Awareness System ............................... 158  
7.8 NSA’s Utah Data Center: A $1.5 Billion Data-Mining and Spy Center .... 158  
7.9 Global Surveillance and Abuse of Power ............................................... 161  
7.10 Edward Snowden’s NSA Leaks and PRISM ........................................... 162  
7.11 Social Networks’ Responses to NSA Leaks and PRISM ...................... 173  
7.12 Reform Government Surveillance and Reset the Net .......................... 176  
Bibliography ................................................................................................. 177

#### 8 A Two-Way Street of Total Information Awareness

8.1 It’s a Small World, with CCTVs .............................................................. 183  
8.2 Facebook Nation: Total Information Awareness ..................................... 184  
8.3 Surveillance Satellites, Tracking Devices, Spyware, and Drones ............ 186  
8.4 A Two-Way Street of Total Information Awareness ............................. 189  
8.5 No Doomsday for the Internet ................................................................. 191
8.6 Web 2.0 for Intelligence Community: Intellipedia, A-Space, Deepnet ................................................................. 192
Bibliography ................................................................. 193

Part IV Cybersecurity: History, Strategies, and Technologies

9 Cyber Warfare: Weapon of Mass Disruption .............................. 201
  9.1 Weapon of Mass Disruption .............................................. 202
  9.2 Financial Disruption .................................................... 203
  9.3 Infrastructure Disruption .............................................. 206
  9.4 Government and Military Disruption ................................. 211
  9.5 Shodan and the Internet of Things ................................... 215
  9.6 Backdoors and Counterfeit Parts .................................... 217
  9.7 Proliferation of Cyber Weapons and Reverse Engineering ....... 219
  9.8 Cyber Espionage and Escalation of Cyber Warfare ................. 220
  9.9 Cyber Cold War ....................................................... 223
  9.10 Psychological Cyber Warfare ....................................... 224
  9.11 Cyber Terrorism and Digital Pearl Harbor ......................... 225
  9.12 Sony-pocalypse: from Cyber Attacks to Cyber Terrorism ....... 227
  9.13 Good, Bad — Internal/External — People Put an End to Business as Usual (A Commentary by Andy Marken) ........ 231
Bibliography ..................................................................... 238

10 Cyber Attacks, Prevention, and Countermeasures ....................... 249
  10.1 Cybersecurity Acts ..................................................... 250
  10.2 Cybersecurity Initiatives: CNCI, NICE, Presidential Executive Order ................................................................. 251
  10.3 National Cyber Security Awareness Month (NCSAM) ......... 252
  10.4 Mitigation from Denial of Service (DoS, DDoS, DRDoS) Attacks ................................................................. 253
  10.5 Data Breach Prevention ................................................ 255
  10.6 Fighting Back Against Phishing and Spoofing ..................... 262
  10.7 Password Protection and Security Questions ..................... 264
  10.8 Software Upgrades and Security Patches ......................... 267
  10.9 Fake Software and Free Downloads ................................ 268
  10.10 Smartphone Security Protection .................................... 270
  10.11 Cybersecurity Awareness: Everyone's Responsibility .......... 274
Bibliography ..................................................................... 276

11 Cybersecurity Training in Medical Centers: Leveraging Every Opportunity to Convey the Message ......................... 287
Ray Balut and Jean C. Stanford
  11.1 Introduction ............................................................. 287
  11.2 Healthcare Cyber Attacks ............................................. 288
  11.3 Value of Medical Data to Cybercriminals ......................... 288
## Contents

### 11.4 Major Threats to Medical Data in Clinical Environments 289
### 11.5 Training Resources 290
### 11.6 Training Users to Prevent Cyber Breaches 291
### 11.7 User Communities and Current Training Methods 292
### 11.8 Types of Training Offered and Training Environment 295
### 11.9 Innovative Approaches 297
### 11.10 Conclusion 299

Bibliography 299

### 12 Plan X and Generation Z 301

12.1 Plan X: Foundational Cyberwarfare 302
12.2 Cyber Battlespace Research and Development 306
12.3 National Centers of Academic Excellence in Cyber Operations 308
12.4 Generation Z, Teen Hackers, and Girl Coders 309
12.5 DEF CON Diversity Panel and IT Girls 2.0 (a Commentary by Emily Peed) 313
12.6 Control the Code, Control the World 314

Bibliography 316

### Part V Cybersecurity: Applications and Challenges

### 13 Artificial Intelligence and Data Mining 323

13.1 Artificial Intelligence: From Hollywood to the Real World 323
13.2 Intelligent CCTV Cameras 325
13.3 Data Mining in the Age of Big Data 326
13.4 Knowledge Representation, Acquisition, and Inference 327
13.5 Dynamic Mental Models 329
13.6 Modeling Human Problem Solving 330
13.7 Structural Topology and Behavioral Causality 331
13.8 Component Clustering and Decoupling 331
13.9 Analytical Models and Experiential Knowledge 332
13.10 The DM² Algorithm 332
13.11 AI Applications in Counterterrorism 336
13.12 Massively Multi-Participant Intelligence Amplification (MMPIA) 337

Bibliography 338

### 14 Gamification of Penetration Testing 343

Darren Manners

14.1 Win, Lose, or Something Else 343
14.2 Short and Long Engagements 344
14.3 A Game Already? 344
14.4 The Future: Continuous Penetration Testing 346

Bibliography 347
15 USB Write Blocking and Forensics ........................................ 349
   Philip Polstra
   15.1 Introduction ..................................................... 349
   15.2 Brief History .................................................. 349
   15.3 Hardware ...................................................... 350
   15.4 Software ...................................................... 350
   15.5 Summary of USB Basics ....................................... 355
   15.6 USB Mass Storage Basics ..................................... 355
   15.7 Making Forensics Images and Duplicates ..................... 360
   15.8 Blocking USB Writes ......................................... 370
   15.9 USB Impersonation .......................................... 406
   15.10 Leveraging Open Source ..................................... 419
   15.11 BadUSB ...................................................... 427

16 DARPA’s Cyber Grand Challenge (2014–2016) ..................... 429
   16.1 Cyber Grand Challenge Kick-off .............................. 429
   16.2 Costly Software Bugs ......................................... 435
   16.3 Disastrous Arithmetic Errors ................................ 437
   16.4 DEF CON Capture the Flag .................................... 438
   16.5 DESCARTES (Distributed Expert Systems for Cyber Analysis,
           Reasoning, Testing, Evaluation, and Security) ........ 438
   16.6 DESCARTES Overview ......................................... 448
   16.7 DESCARTES Automation Strategy ............................. 453
   16.8 The DESCARTES Chronicle ................................... 454
Bibliography .......................................................... 455

Index ................................................................. 457