NUMBERS
9/11 attacks
  countermeasure lack, 74
new forms of attack and, 74
Pearl Harbor comparison, 70–71
Tillman, Mark, 113

A
ABAB design, 208
ABC (antecedent-behavior-consequence sequence), 3
BAF (Behavior Analysis Form), 209–210
behavior modeling and, 175–176
patterns of behavior and, 170
predicting behavior and, 170
abnormal behavior, behavior analysis and, 5
acts of anger, surrogate targets and, 98
adversarial behavior
  AuBA, global, 190–192
  consistency, 319–320
data gathering for understanding, 187–190
historical data, 191–192
influencing/preventing, 178–180
predicting, 178, 194–196
transitions, 434–435
adversaries, sophistication, 142–144
al-Qaeda
  attack targets, 41–42
  basic tenets, 36
  behavior analysis, 43–44
fatwas, 42–43
franchise comparison, 40–41
future targets, 44
  group dynamics, 41–42
Israel common enemy with Hezbollah, 45
leadership, 40–41
deaths, 71
motivation, 42
structure, 41
ThemeMate, 37–41
as top terrorist threat to U.S., 71
U.S. citizen members, 238
war and, 42–43
amateur insider threat, 287–288
Ames, Aldrich, 24, 240, 245–246
Analysis ToolPak (Microsoft), 340–344
ankle biters, 116
anomalies, 266–267
anticipating, 269–270
anomaly detection
  AuBA and, 456–457
  criminal behavior, 272–273
  advantages, 267
  disadvantages, 267–268
  methods, 269
  normal definition, 126–128
  reactivity of network security, 293–294
terrorism, 270–271
anonymity, hackers and, 18–19
Anonymous cyber threat, 51
antecedent-behavior-consequence sequence. See ABC (antecedent-behavior-consequence sequence)
antecedents, 3
area of influence and, 171–172
AuBA, 366–367
behavioral chain, 8
environmental, 167
militant action and, 72
stability, 172
anticipating events, 445–446
APTs (advanced persistent threats), 17
China's Google attack (Operation Aurora), 289
growth, 150
insider threat, 292–293
McAfee definition, 51
area of influence, antecedents and, 171–172
ARPANET, 115
asymmetric warfare, 66
anticipating future, 145–146
terrorists, 106
ATM thefts, ThemeMate and, 341–342
atomic bomb, 64–65
attacks
detection, first-time attacks, 107–109
element of surprise in, 105–106
informed security and, 155–156
first-time behavior analysis and, 273
identifying, 263–266
as focus rather than people, 93
handshake connection, 126
unanticipated, 128
terrorism, 146–147
unknown, identifying, 263–266
zero-day, 108–109, 123
signature detection and, 169
AuBA (automated behavior analysis), 11
adversarial behavior, 175–176
global, 190–192
influencing/preventing, 178–180
predicting, 178
analytical brain extension, 402–404
ANNs (artificial neural networks), 156
anomaly detection, 456–457
antecedents, 366–367
anticipating events, 445–446
applied behavior analysis, extensions, 181
applying, 351–352
cyber attacks, 411–412
future threat, 406–407
network security, 412–422
AutoAnalyzer, 177
as predictive tool, 217
automated summarization, 29–32
automation, 481–485
methodology, 485–491
behavioral science automation, 201–205
behaviorprints, 118–119, 295
signature detection and, 326–327
state-sponsored threat, 322–325
benefits, 378
BPN (back propagation network), 157
CheckMate, 19
adversarial behavior, 178
deception measure, 134
domestic threat, 232
expertise measure, 134
external threats, 132, 413–417
first-time attack detection, 108–109
human behavior and, 173
network security, 396–399
phishing module, 187
predictive application, 418–419
proactive application, 417–418
protective application, 419–420
real-world event prediction, 198–199
signature detection, future signatures, 263
testing, 400–402
threat, early identification, 173–174
validation, 400–402
clinical case examples, 472–479
analysis and solution, 475–476
computer science automation, 201–205
confusion matrix, 313
current security fixes, 468–469
error reduction in manual predictive modeling, 87–89
extensions, 225–227
features, 378
first-time attack detection, 107–108
future, 469–470
global security and, 180–182
methodology, 312–313
modeling methods, 311–317
human behavior
assessment of threats from network packets, 135–136
information gathering, 430–432
document selection, 432–433
missing data, 435–440
InMate, 18–19, 83, 132–133
adversarial behavior, 178–179
Deception rating, 133
domestic threat, 232–233
human behavior and, 173
insider treat, 420–422
Intent ratings, 133
network security, 396–397, 399–400
real-world event prediction, 198–199
L-1 (Leaving-One-Out) validation, 200–201, 207, 312–313
model focus, 227–228
modeling
correlations, 441–442
frequency, 441
judgment, 441
predicting with model, 389–390
predictive modeling and, 395
results from multiple, 444–445
sensor output, 393–402
network security, 275–276
automated characterization, 447–448
network tools, 82
overview, 358–359
pattern classification, 156–158
predictive analysis engines, 296–297, 379–380
AutoAnalyzer and, 491–494
predictive applications, 109–111
predictive indicators, 366–367
predictive modeling, 252–253
proactive action, 252–253, 458–459
procedures, 224
reasons for development, 176–177, 349
signature detection, 455–456
SPR (statistical pattern recognition), 156
technological advances and, 354–355
terrorism prediction, 336
text as input, 486–488
theme-guided smart searches, 59–61
ThemeMate, 30–32, 88, 177, 215–216, 341
accuracy, 375–376
al-Qaeda, 37–41
ATM thefts, 341–342
AutoAnalyzer and, 217–220, 377–379
compression, 366
cultural issues, 352
cyber threats, open source models, 390–393
document processing, 364–366
language and, 363–364
modeling, 384–393
news articles, 387–388
Old Testament trial, 365
overview, 359–360
as predictive tool, 216–217
processing text corpus, 488–491
significant features, 360–361
theme components file, 385, 436
ThemeMate/ AutoAnalyzer combination, 217–220
tools versus applications, 383
versatility, 423
AuBASME (AuBA Subject Matter Expert), 200
automated behavior analysis, 313–317
CBRN and, 315–317
missing data and, 436–437
predicting behavior and, 437–440
predictive modeling and, 205–206
qualifications, 205–206
AutoAnalyzer, 88–89, 177, 359
data array construction, 367–372
internal workings, 493–494
neural networks and, 374
overview, 373–374
predictive engines, 491–494
as predictive tool, 217
ThemeMate combination, 217–220
integration, 377–379
automation
bias removal and, 350–351
ThemeMate and, 361–362

B

BAAs (Broad Area Announcements), 379
BAF (Behavior Analysis Form), 209–210
Bandura, Albert, 9
modeling behavior, 103–104
Bayesian analysis, 344
behavior
acquiring through modeling, 103–104
consequences, 165
definition, 167
different results from same event, 95–96
insider threat and, 283–292
motivation and, 36
patterns (See patterns of behavior)
predicting by past accounts, 35, 75, 170
behavior analysis, 4
abnormal behavior, 5
al-Qaeda, 43–44
antecedent, 167
automation, 350–351
behavior principles and, 166–169
bias, removing, 15
Bundy, Ted, 6, 11–15
complexities of malicious behavior, 13–15
consequences, 167
cultural perspective, 174–175
copycat behavior, 9
first-time attacks, 273
hackers, 6
Hezbollah, 48–50
human bias and, 345–349
identifying, 349–350
individuals
advantages/
 disadvantages, 25–26
The Chameleon, 27–28
The Loner, 27
The Social Misfit, 28–29
variances in individuals, 26–27
methodology, 163–166
observation, 168, 188–189
predicting behavior and, 167
Reid, Richard, 6–11
subjectivity, removing, 15
technology enhancement and, 134
behavior modeling, 175–176
ABC and, 175–176
predictive modeling, 175
behavior principles, behavior analysis and, 166–169
behavioral chain, Richard Reid, 8
behavioral methodologies, 207–208
ABAB design, 208
manual approach, 209–211
computer tools support, 211–213
within-subject design, 208
behavioral science, 325–326
paradigm shift, 459–463
technology and, 332–333
computer speed and memory, 337–345
polls, 333–334
software need, 340–345
stock market prediction, 334–336
behavior-based analytics, 192–194
behaviorprints (AuBA), 118–119, 295
signature detection and, 326–327
state-sponsored threat, 322–325
bias, 376–377
analysis and, 345–349
automation and, 350–351
behavior analysis, 15
identifying, 349–350
ThemeMate, 376–377
biological attack, 85
global threat, 308
threat, overview, 85–86
Black Hat meetings of hackers, 56
bombings
dirty bombs, 86–87
suicide, 73
suitcase bombs, 309
BPN (back-propagation neural network), 428
Branch Davidians, Timothy McVeigh and, 93–94
brush pass/digital brush pass, 250
bullying, 98
adult involvement, 102
gender issues, 102
Bundy, Ted, 6, 11–15
as Chameleon, 27–28
causation, inferring, 372
causes, terrorists and, 94
CBRN (chemical, biological, radiological, and nuclear) threats, 84–85, 147–148
AuBASME and, 315–317
biological attack, 85
chemical attack, 84
global threat, 307–308
biological, 308
chemical threat, 307–308
nuclear, 309–310
radiological, 308–309
nuclear attack, 85
radiological attack, 85
CERT team, 119
CheckMate, 18
adversarial behavior, 178
deception measure, 134
domestic threat, 232
expertise measure, 134
external threats, 132, 413–414
automated human behavior assessment, 415–417
human behavior, 414
first-time attack detection, 108–109
human behavior and, 173
network security, 396–397
intrusion protection system, 397–399
phishing module, 187
predictive application, 417–418
proactive application, 417–418
protective application, 419–420
<table>
<thead>
<tr>
<th>Index</th>
<th>C–C</th>
<th>505</th>
</tr>
</thead>
<tbody>
<tr>
<td>SPSS (Statistical Package for the Social Sciences), 345</td>
<td>criminal behavior, anomaly detection, 272–273</td>
<td></td>
</tr>
<tr>
<td>statistical packages, 344–345</td>
<td>criminal signatures, 260–262</td>
<td></td>
</tr>
<tr>
<td>surveillance and, 261–262</td>
<td>al-Qaeda, 261</td>
<td></td>
</tr>
<tr>
<td>tools, 338–340</td>
<td>Bundy, Ted, 261</td>
<td></td>
</tr>
<tr>
<td>confusion matrix, 313</td>
<td>cultural issues, 352</td>
<td></td>
</tr>
<tr>
<td>consequences, 3, 165</td>
<td>cultural perspectives consequences, 174–175</td>
<td></td>
</tr>
<tr>
<td>behavioral chain, 8</td>
<td>ThemeMate and, 352</td>
<td></td>
</tr>
<tr>
<td>cultural perspective, 174–175</td>
<td>cyber attackers.</td>
<td></td>
</tr>
<tr>
<td>definition, 167</td>
<td>See hackers</td>
<td></td>
</tr>
<tr>
<td>environmental conditions, 167</td>
<td>cyber attacks</td>
<td></td>
</tr>
<tr>
<td>suicide bombers, 174</td>
<td>anomaly detection, 105–106</td>
<td></td>
</tr>
<tr>
<td>timing, 172</td>
<td>AuBA application, 411–412</td>
<td></td>
</tr>
<tr>
<td>context in predicting behavior, 426–428</td>
<td>global threat and, 301</td>
<td></td>
</tr>
<tr>
<td>contingency management, 188</td>
<td>state-supported, 304–306</td>
<td></td>
</tr>
<tr>
<td>control, lack of in threats, 70</td>
<td>objectives, 79</td>
<td></td>
</tr>
<tr>
<td>coordinated group cyber threats, 50–51</td>
<td>signature detection, 105–106</td>
<td></td>
</tr>
<tr>
<td>Anonymouse, 51</td>
<td>signature detection, known attacks and, 256–262</td>
<td></td>
</tr>
<tr>
<td>copycat behavior, 9</td>
<td>terrorists, unanticipated, 104–107</td>
<td></td>
</tr>
<tr>
<td>correlations, 370</td>
<td>unanticipated, 128</td>
<td></td>
</tr>
<tr>
<td>country-level threats</td>
<td>U.S. as target, 138–139</td>
<td></td>
</tr>
<tr>
<td>assault, 68</td>
<td>cyber theft</td>
<td></td>
</tr>
<tr>
<td>biological, 68</td>
<td>group behavior, 187</td>
<td></td>
</tr>
<tr>
<td>chemical, 68</td>
<td>hackers and, 23–25</td>
<td></td>
</tr>
<tr>
<td>cyber attack, 67</td>
<td>national security, probability, 142</td>
<td></td>
</tr>
<tr>
<td>cyber theft, 67</td>
<td>phishing, 187</td>
<td></td>
</tr>
<tr>
<td>explosives, 68</td>
<td>state-supported terrorism and, 67</td>
<td></td>
</tr>
<tr>
<td>IED explosives, 68</td>
<td>cyber threats</td>
<td></td>
</tr>
<tr>
<td>national infrastructure, 64–69</td>
<td>Anonymous, 51</td>
<td></td>
</tr>
<tr>
<td>nuclear, 68</td>
<td>blacklist, 54</td>
<td></td>
</tr>
<tr>
<td>radiological, 68</td>
<td>coordinated groups, 50–51</td>
<td></td>
</tr>
<tr>
<td>suicide attacks outside U.S., 68</td>
<td>ThemeMate, open source models, 390–393</td>
<td></td>
</tr>
<tr>
<td>technology and, 63–64 warfare</td>
<td>whitelist, 54</td>
<td></td>
</tr>
<tr>
<td>asymmetric warfare, 66</td>
<td>Cyber War: The Next Threat to National Security and What to Do About It (Clarke and Knake), 304</td>
<td></td>
</tr>
<tr>
<td>atomic bomb, 64–65</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
D
Dahmer, Jeffrey, 6
DARPA, 115
data arrays (AutoAnalyzer), 367–372
dead drop, 241, 244
digital dead drop, 249–250
death by cop, public violence and, 101
deception
CheckMate and, 18
e-mail, 251
insider threat and, 290–291
Department of Homeland Security, formation, 66
digital brush pass, 250
digital cutouts, 251
digital dead drop, 249–250
dirty bombs, 86–87, 308–309
disgruntled employees
insider threat and, 241
workplace shootings, 101
document processing in ThemeMate, 364–366
document selection for basic corpus, 432–433
domestic threat, 231
CheckMate, 232
foreign threat
differentiation, 236–239
InMate, 232, 233
insider threat, 232
insider description, 239–240
sabotage, 242–243
spies, 239–240
targeting and, 234
terrorism, 235
surveillance and, 237–238
DOS (denial-of-service) attack, 16, 23
foreign attack on U.S. networks, 55
dual terrorist attack, 22–23
E
element of surprise in an attack, 105–106
informed security and, 155–156
e-mail, malware, 143, 251
employees
disgruntled, workplace shootings, 101
insider threat, 241
environment
adaptation to, 164
antecedents, 167
consequences, 167
interactions and, 172
meaning in, 164
Skinner, B.F., 164
studying, 165
variables, 169–170
Espionage Against the United States by American Citizens 1947–2001 (Herbig and Wiskoff), 246
Excel, 212–213, 340–344
explosives
dirty bombs, 86–87
IEDs, 73
suicide bombings, 73
suitcase bombs, 309
external data, predicting behavior and, 433–434
F
false negatives in signature detection, 123–124
financial markets, national security and, 152–153
first-time attacks
behavior analysis and, 273
detecting, 107–109
identifying, 263–266
focus words (ThemeMate), 38
food terrorism, 148
foreign threat/domestic threat differentiation, 236–239
foreign threats to network security, 82–83
forensics, 319–320
motivation and, 320
forensics (network), 317–319
analysis, 318
attack identification, 173
collection, 318
examination, 318
Ranum, Marcus, 273
reporting, 319
signature detection, 122
Fort Hood shootings, 234
future signatures, 453–454
G
Gallup Poll, 334
genius portrayal of hackers, 115
global adversary behavior, AuBA and, 190–192
global security, AuBA and, 180–182
global threat
AuBA modeling methods, 311–312, 440–442
correlations, 441–442
frequency, 441
judgment, 441
methodology, 312–313
multiple models, 442–444
CBRN
biological threat, 308
chemical threat, 307–308
nuclear, 309–310
radiological, 308–309
cyber attacks, 301
state-supported, 304–306
interconnectedness and, 299–300
state-sponsored, 300–301
cyber attacks, 304–306
organized support, 301–306
cyber theft, 187
MO (modus operandi), 186
objectives, 185
terrorists, motivation emphasis, 186
threat, move to action, 185–186
groups
characteristics, 35
description, 36
versus individuals, 29
individuals motivations, 97
members, behavior analysis and, 4
motivation, malicious intent/behavior and, 36
pressure from other members, 36

H
hackers, 6, 15–16
ankle biters, 116
anonymity and, 18–19
APTs (advanced persistent threats), 17
Black Hat meetings, 56
DOS (denial-of-service) attack, 16, 23
genius portrayal, 115
motivation, 20–21
national network security, 114–117
power of disruption, 21–23
recognition desires, 116
script kiddies, 116
state-supported terrorism and, 67
target detachment, 19–20
theft and, 23–25
threat identification, 16–17
hacking, malicious intent, 116
handshake connection, 121
attackers and, 126
Hanssen, Robert, 24, 241, 245
dead drop, 244
Harris, Eric, 92
Hasan, Nidal, 234
Hawkins, Robert, 92
Herbig, Katherine L., Espionage Against the United States by American Citizens 1947–2001, 246
Hezbollah, 45
behavior analysis, 48–50
consistency, 46–48
forms, 46
Iranian support, 66
Iranian ties, 45
Israel
common enemy with al-Qaeda, 45
Katyusha rockets, 48
motivation, 47
Nasrallah, Sayyed Hasan, 46
organization, 45–46
ThemeMate, 45
HFT (High Frequency Trading), 334–336
hiding information, 285–286
historical data, 199
adversarial behavior, 191–192
missing, 199–200
hollow-point ammunition, 28–29
human behavior
CheckMate and, 173
InMate and, 173
network security and, 130–133
packet switching networks and, 131–132
threats assessment from network packets, 135–136

I-J
IEDs (improvised explosive devices), 73
IEP (individualized education plan), 189–190
individual behavior modeling advantages/disadvantages, 25–26
The Chameleon, 27–28
The Loner, 27
The Social Misfit, 28–29
variances in individuals, 26–27
individual versus group, 29
information gathering, predicting behavior and, 430–432
document selection, 432–433
missing data, 435–440
information hiding, 285–286
informed security, element of surprise and, 155–156
infrastructure
computer/network dependencies, 140
country-level threats and, 64–69
future attacks, MOs, 140–141
National Infrastructure Protection Plan, 140
InMate, 18, 83, 132–133
adversarial behavior, 178–179
Deception rating, 133
domestic threat, 232–233
human behavior and, 173
insider treat, 420–422
Intent ratings, 133
network security, 396–397
misuse detection system, 399–400
real-world event prediction, 198–199
insider threat amateurs, 287–288
deception and, 290–291
disgruntled employees, 241
domestic threat, 232
flags, 282
hiding information, 285–286
ideology changes, 282–283
insider behaviors, 283–292
insider description, 239–240
Manning, Bradley, 118
methods of operation, 284–285
MOs, 284–285
motivations of insiders, 281–284
network security, 82–83, 117–118
InMate, 420–422
network thief, behavior of, 291–292
professionals, 288–290
protection, trends in, 292–295
sabotage, 242–243
significance of, 279–281
spies, 240–242
tradecraft
known tradecraft, 243–244
new tradecraft, 246–247
traditional-new hybrid, 247
without intent, 278
insiders, definition, 278–279
intent, motivation and, 36
interconnectedness
global threat and, 299–300
growing dependency, 138–139
internal threats
InMate, 132–133
network security, 277–278
Internet, development, 249
ISC (Internet Storm Center), 119

known attacks, network security, signature
detection, 256–262
known tradecraft, 243
brush pass, 244
steganography, 245

L
language, ThemeMate and, 363–364
Libyan state-supported terrorism, 303–304

M
mailbox limit exceeded spear phishing scam, 262
malicious hackers as geniuses, 115
malware, 143
e-mail, 251
Manning, Bradley insider threat and, 118
methods compared to Jonathon Pollard, 286
tradecraft, 247
manual approach to behavioral methodology, 209–211
computer tools support Excel, 212–213
MatLab, 211
SPSS, 211
Maslow, Abraham, 149, 163–164
Maslow’s Hierarchy of Needs, 149, 163–164
McVeigh, Timothy, 92
Branch Davidians and, 93–94
media
depiction of violence, 103
“villain with technology” movie genre, 142–143
Microsoft Analysis ToolPak, 340–344
militant action, 72
miniaturization, theft and, 247
Minority Report, 453
missing data, 435–440
misuse detection system (InMate), 399–400
MNLF (Moro National Liberation Front), 304
MO (modus operandi), 46
eye for an eye principle, 50
group behavior, 186
insiders, 284–285
modeling behavior, 103–104, 175–176
predictive modeling, 175
motivation
al-Qaeda, 42
Bundy, Ted, 12–13
criminal signatures, 260–262
forensics and, 320
hackers, 20–21
Hezbollah, 47
insider threats, 281–283
flags, 282
ideology changes, 282–283
revenge, 283–284
malicious intent/behavior and, 36
method pairing, 233
Reid, Richard, 8–9
movement tracking, sensor output and, 394–396

N
Nasrallah, Sayyed Hasan, 46
national infrastructure
country-level threats and, 64–69
future attacks, probable activity, 141–142
National Infrastructure Protection Plan, 140
national network security, hacking, 114–117
national security
adversary’s capabilities, 142–144
Americans’ worldwide safety, 150–152

K
Kaczynski, Theodore (“Ted”), 27
Kikumura, Yu, 270
Klebold, Dylan, 92
Knake, Robert K., Cyber War: The Next Threat to National Security and What to Do About It, 304
knowledge engineers, 314
cyber theft, probability, 142
financial markets, 152–153
future attacks
MOs, 140–141
probable activity, 141–142
informed security, 155–156
networks, growing dependency, 138–139
NEW (new emergent weapon), 141
proactive methods, 154
moving from reactive, 154–155
water/food resources, 148–150
WMDs (weapons of mass destruction), 147–148
NEO, 280
network attacks. See cyber attacks
network behavior, human behavior augmentation, 130–131
network security, 78–79
9/11 attacks, 464
anomaly detection, 80, 105–106, 124–128, 266–267, 271–272
advantages, 267–268
disadvantages, 267–268
methods, 269
normal definition, 126–128
anticipating unknown, 106–107
attack detection technology, 81
AuBA application, 412–413
automated characterization, 447–448
CheckMate, 413–420
InMate, 420–422
AuBA network tools, 82, 275–276
bail out, 464–465
CERT team, 119
CheckMate, 396–399
current, 79–82, 465–469
current technology, 83–84
cyber attacks, objectives, 79
economy fall, 464–465
effectiveness, 150
external threats,
CheckMate, 132
first-time attack identification, 263–266
fixing ineffective, 128–132
foreign threats, 82–83
forensics, 273, 317–319
analysis, 318
collection, 318
examination, 318
reporting, 319
future protection technology, 133–134
increases in damage and threat, 117–120
InMate, 396–397
misuse detection system, 399–400
insider threat, 82–83
internal threats, 277–278
InMate, 132–133
national, hacking, 114–117
paradigm shift, 294–295
proactive, 458–459
proactive state, 129–130
reactivity, 81, 293
anomaly detection and, 293–294
AuBA and, 295
shifting to proactive capabilities, 294–295
signature detection and, 293
SANS Internet Storm Center, 119
signature detection, 80, 105–106, 120–122, 258–259
false negatives, 123–124
forensics, 122
known attacks, 256–262
problems with, 257–258
Snort rule, 260
terrorism comparison, 259–260
Sophos Security Threat Report 2011, 255
Soviet Union and, 463–464
surrender principle, 80
unanticipated attacks, 128
unknown attack identification, 263–266
zero-day attacks, 123
networks
handshake, 121
national security, growing dependency, 138–139
packet switching network, 121
human behavior assessment of threats on, 135–136
human intent identification, 131–132
predictive modeling and, 395
neural networks and AutoAnalyzer, 374
NEW (new emergent weapon), 141
new tradecraft, 246–247
news articles in ThemeMate, 387–388
nuclear attack, 85
global threat, 309–310
nuclear warheads, 65
observation in behavior analysis, 168, 188–189
Occupy Wall Street movement, 20, 409–410
Oklahoma City bombing, 92
Oklahoma City National Memorial, 95
Old Testament trial, 365
Omaha, Nebraska, Westroads mall shooting, 92
open source cyber threat models (ThemeMate), 390–393
Osama bin Laden, 31–32
al-Qaeda leadership and, 71
overview, 359–360

P-Q
packet switching network, 121
bundles of activity, 131
human intent
identification, 131–132
predictive modeling and, 395
threats, human behavior assessment, 135–136
Padilla, Jose, 309
Pakistan state-supported terrorism, 303–304
paradigm shift in network security, 294–295
behavioral science-based, 459–463
past information predicting behavior and, 274
usage updates, 274–275
pattern classification (AuBA), 156–158
patterns of behavior, ABC and, 170
*Patterns of Global Terrorism* (State Department), 235
Pearl Harbor, 9/11 comparison, 70–71
penny stock investments, 350
PFLP (Palestine Front for the Liberation of Palestine), 304
phishing CheckMate module, 187
spear phishing, 262
PLO (Palestine Liberation Organization), 304
Pollard, Jonathon, 246
methods compared to Bradley Manning, 286
polling, 333–334
portable computing, advent of, 248–249
pre-crime methods, 453–454
predicting behavior adversarial, 178, 194–196
analysis groups, 429–440
individuals, 429–440
antecedents and, 170
stability and, 172
anticipating events, 445–446
applied behavior analysis and, 167
area of influence and, 172
AuBASME and, 216–217
AutoAnalyzer, 217
consequences and, 170
timing, 172
counterterror, 426–428
environment, interactions with, 172
external data, 433–434
future signatures, 453–454
historical information, 199–200
information gathering, 430–432
manual methods, 331–332
new adversary threat, 452–453
past accounts, 35, 75, 170, 184, 199
past accounts and, 274
ThemeMate, 216–217
predicting events, 198
prediction definition, 196
methodology *versus* statistics, 197
reliability, 197
validity, 197
predictive applications
AuBA, 109–111
False Negative, 195
False Positive, 195
True Negative, 195
True Positive, 195
predictive indicators (AuBA), 366–367
predictive modeling, 175
data processing, 206–207
input data, 204–205
AuBASME, 205–206
historical events, 205
model construction, 203–207
model development, 206–207
SMEs (subject matter experts), 204
testing, 207
validation, 207
predictive security model, terrorism and, 77
predictive surveillance, 225
presidential polls, 333–334
proactive methods for national security, 154
moving from reactive, 154–155
proactive security, 458–459
professional insider threat, 288–290
protocol anomaly detection, 105
public violence, 92–104
death by cop, 101
precursors, 101
as suicide mission, 101–102
surrogate targets in acts of anger, 98
workplace shootings, 101
R
radiation, dirty bombs, 86–87
radiological attack, 85
dirty bombs, 86–87
global threat, 308
rare event prediction, 306–310
reactivity of network security, 81
Reid, Richard, 6–11
reliability, definition, 311
repeated behavior, signature detection and, 257
resources, national security, 148–150
revenge, insider threat and, 283–284
RFP (Requests for Proposal), 379
Russian state-supported terrorism, 303

S
sabotage, 242–243
sampling, 333–334
SANS Internet Storm Center, 119
Scheuer, Michael, 31–32
script kiddies, 116
security global, AuBA and, 180–182
malicious behavior reduction and, 76–77
national (See national security)
network security, 78–79
anomaly detection, 80, 124–128
anticipating unknown, 106–107
attack detection technology, 81
AuBA network tools, 82
current, 79–82
current technology, 83–84
cyber attack objectives, 79
fixing ineffective, 128–132
foreign threats, 82–83
future protection technology, 133–134
increases in damage and threat, 117–120
insider threat, 82–83
national, 114–117
proactive state, 129–130
reactivity, 81
signature detection, 80, 120–124
surrender principle, 80
unanticipated attacks, 128
zero-day attacks, 123
predictive security model, terrorism and, 77
public places, 99
sensor output, 393
movement tracking, 394–396
Shia Muslims, Hezbollah, 45
shoe bomber. See Reid, Richard
signature detection AuBA and, 455–456
behaviorprints (AuBA) and, 326–327
CheckMate, future signatures, 263
combinatorial explosion and, 263
criminals, 260–262
al-Qaeda, 261
Bundy, Ted, 261
network security, 80, 105–106, 120–122, 258–259
false negatives, 123–124
forensics, 122
known attacks, 256–262
problems with, 257–258
repeated attacks and, 169, 257
Snort rule, 260
terrorist attacks, 141
zero-day attacks, 169
reactivity of network security, 293
terrorism, 259–260
significant features, 360–361
Silk Stalkings, 244
Skinner, B.F., environment and, 164
SME (subject matter expert) descriptions, 4
predictive modeling and, 204
qualifications, 205–206
Snort rule, network security, 260
Sophos Security Threat Report 2011, 255
spear phishing, 262
speed, 375
spies, 240–242
spy gear ease of purchase, 246–247
state-sponsored threat, 300–301
behaviorprints (AuBA), 322–325
cyber attacks, 304–306
evidence gathering, 321–322
organized support, 301–302
foreign-supported terrorist attacks, 302–304
state-sponsored terrorism, 66
threat types, 67–68
statistical software packages, 344–345
steganography, 245
insider threat and, 286
notes in images, 251
stimulus control, 219
stock market predictions HFT (High Frequency Trading), 334–336
penny stock investments, 350
student suicide, 98
gender differences, 102
warning sign awareness, 102–103
subjectivity, behavior analysis, 15
suicide
  public violence and, 101–102
  student, 98
    gender differences, 102
  warning sign awareness, 102–103
suicide bombings, 73
  consequences, 174
suitcase bombs, 309
Sunni Islam, 41
surprise in an attack, 105–106
surrender principle, 80
surveillance
  criminal activity and, 261–262
  domestic terrorism and, 237–238
  predictive, 225
T
Taleb, Nassim Nicholas, The Black Swan: The Impact of the Highly Improbable, 306
technology. See also computing power
  attack detection, first-time attacks, 107–109
  behavior analysis
    enhancement and, 134
  behavioral science and, 332–333
  computer speed and memory, 337–345
  polls, 333–334
  software need, 340–345
  stock market prediction, 334–336
  country-level threats and, 63–64
  future capabilities, 118–119, 133–134
  versus human suicide bomber, 73
  network security, 83–84
  uses, 219–223
“villain with technology” movie genre, 142–143
terrorism
  al-Qaeda
    top threat to U.S., 71
  U.S. citizens members, 238
  anomaly detection, 270–271
  asymmetric warfare, 106
  attack prevention in U.S., 75–77
  AuBA prediction, 336
  causes, 9
  current threats to U.S., 70–75
  cyber attacks, unanticipated, 104–107
  domestic, 235
  surveillance and, 237–238
  dual attack, 22–23
  food terrorism, 148
  IEDs (improvised explosive devices), 73
  increase ineffectiveness, 66
  security, predictive security model, 77
  signature detection, 259–260
  specific attack threat, 69–70
  state-supported, 66, 302–303
  Libya, 304
  Pakistan, 303–304
  Russia, 303
  threat types, 67–68
  unanticipated attacks, 146–147
  weapons of mass destruction and, 71
  terrorists
    causes, 94
    group formation, 75
    group motivation emphasis, 186
    repeat perpetrators, 75
    sharing resources, 74
  U.S. citizens
    acting alone, 408–409
    al-Qaeda, 238
    foreign agents, 408
    leaving country, 408
    testing, CheckMate, 400–402
    text as input, 486–488
    text summarization (compression), 366
    The Black Swan: The Impact of the Highly Improbable (Taleb), 306
    The Chameleon, 27–28
    theft. See also cyber theft
      miniaturization and, 247
      network thieves, 291–292
      tradecraft
        known tradecraft, 243–244
        new tradecraft, 246–247
        traditional-new hybrid, 247
      theme-guided smart searches, 59–61
    ThemeMate, 30–32, 88, 177, 215–216
      accuracy, 375–376
      al-Qaeda, 37–41
      ATM thefts, 341–342
      AutoAnalyzer
        combination, 217–220
        integration, 377–379
        cyber threats, open source models, 390–393
        modeling
          adversarial groups, 386–387
          adversaries, 386–387
          model testing, 388–389
          text accounts from past behavior, 384–393
          news articles, 387–388
          processing text corpus, 488–491
          theme components file, 385, 436
          themes, 156–157
          threat identification
            early, CheckMate, 173–174
hackers, 16–17
threats
analysis, 184
biological attack,
overview, 85–86
CBRN (chemical,
biological,
radiological, and
nuclear), 84–87
domestic
foreign threat
differentiation,
236–239
insider threat and, 232
targeting, 234
terrorism, 235
external, CheckMate, 132
global
cyber attacks, 301
interconnectedness and,
299–300
state-sponsored threat,
300–306
group behavior, move to
action, 185–186
internal, InMate, 132–133
lack of control and, 70
state-supported
behaviorprints (AuBA),
322–325
evidence gathering,
321–322
tracking
abilities, 118–119
movement, 394–396
tradecraft
known tradecraft,
243–244
brush pass, 244
steganography, 245
new tradecraft, 246–247
traditional-new hybrids,
247
traditional-new hybrid
tradecraft, 247

U
Unabomer, 27
unanticipated attacks, 128
terrorism, 146–147
underwear bomber, 9
unknown attacks,
identifying, 263–266
U.S.
aggressiveness, 99–100
allies against Middle
Eastern militants, 71
cyber attack, as leading
target, 138–139
safety in, 99
terrorism
al-Qaeda as top threat,
71
attack prevention, 75–77
current threats, 70–75
worldwide security for
Americans, 150–152
U.S. citizen terrorists, 407
acting alone, 408–409
al-Qaeda, 238
foreign agent, 408
leaving country, 408

V
validation, CheckMate,
400–402
validity, definition, 311
variables in environment,
169–170
video camera surveillance,
225
video game violence, 103
“villain with technology”
movie genre, 142–143
violence
media depiction, 103
public
death by cop, 101
precursors, 101
as suicide mission,
101–102
surrogate targets in acts
of anger, 98
workplace shootings, 101
reasons for, 99–104
video depiction, 103
Virginia Tech University
shootings, 28–29

W
war, al-Qaeda and, 42–43
warfare, asymmetric
warfare, 66
anticipating future,
145–146
terrorists, 106
water/food resources,
national security,
148–150
weapons of mass
destruction (WMDs)
national security, 147–148
terrorism fear and, 71
Westroads mall shooting
(Omaha), 92
WikiLeaks, insider threat
and, 118
Wiskoff, Martin F.,
Espionage Against
the United States by American
Citizens 1947–2001, 246
within-subject design, 208
words with similar
meanings, 376
workplace shootings, 101
worldwide security for
Americans, 150–152

X-Y-Z
zero-day attacks, 108–109,
123
signature detection and,
169