Contents

Preface xi

List of Figures xiii

List of Tables xv

1 Introduction 1

2 Cyberspace 3

2.1 What is cyberspace? 3

2.2 The impact of cyberspace 6

2.3 Identity and authentication 7

2.4 Encryption 11

2.5 Crime is changing 15

2.6 Policing is changing 17

3 New opportunities for criminality 21

3.1 Unprecedented access to information 21

3.2 Crimes directed against cyberspace 23

3.2.1 Malware 23

3.2.2 Crimes of destruction 27

3.2.3 Monetized cybercrimes 29

3.2.4 Data theft crimes 31

3.2.5 Secondary markets 33

3.3 Crimes that rely on cyberspace 36

3.3.1 Spam, scams, and cons 37
3.3.2 Financial crime 40
3.3.3 Online shopping 40
3.3.4 Crimes against children 42
3.4 Crimes done differently because of cyberspace 42
3.4.1 Disseminating hatred 42
3.4.2 Selling drugs 43
3.4.3 Stalking and crime preparation 45
3.4.4 Digital vigilantes 46
3.5 Money laundering 47
3.5.1 Cash 48
3.5.2 The financial system 49
3.5.3 International money laundering 53
3.5.4 Cryptocurrencies 54
3.6 Overlap with violent extremism 55

4 New ways for criminals to interact 61
4.1 Criminal collaboration 61
4.2 Planning together 63
4.3 Information sharing 64
4.3.1 Sharing techniques 64
4.3.2 Sharing resources 66
4.3.3 Sharing vulnerabilities 66
4.4 International interactions 67

5 Data analytics makes criminals easier to find 69
5.1 Understanding by deduction 70
5.2 Understanding by induction 74
5.3 Subverting data analytics 79
5.4 Intelligence-led policing 81
5.5 Hot spot policing 82
5.5.1 Place 83
5.5.2 Time 85
5.5.3 Weather 86
5.5.4 People involved 87
5.5.5 Social network position 87
5.6 Exploiting skewed distributions 91

6 Data collection 101

6.1 Ways to collect data . . . 101

6.2 Types of data collected . . . 104

6.2.1 Focused data . . . 104

6.2.2 Large volume data . . . 105

6.2.3 Incident data . . . 109

6.2.4 Spatial data . . . 109

6.2.5 Temporal data . . . 110

6.2.6 Non-crime data . . . 111

6.2.7 Data fusion . . . 112

6.2.8 Protecting data collected by law enforcement . . . 114

6.3 Issues around data collection . . . 114

6.3.1 Suspicion . . . 114

6.3.2 Wholesale data collection . . . 116

6.3.3 Privacy . . . 118

6.3.4 Racism and other -isms . . . 118

6.3.5 Errors . . . 119

6.3.6 Bias . . . 120

6.3.7 Sabotaging data collection . . . 123

6.3.8 Getting better data by sharing . . . 124

7 Techniques for data analytics 129

7.1 Clustering . . . 129

7.2 Prediction . . . 137

7.3 Meta issues in prediction . . . 140

7.3.1 Classification versus regression . . . 140

7.3.2 Problems with the data . . . 140

7.3.3 Why did the model make this prediction? . . . 142

7.3.4 How good is this model? . . . 143

7.3.5 Selecting attributes . . . 146

7.3.6 Making predictions in stages . . . 148

7.3.7 Bagging and boosting . . . 149

7.3.8 Anomaly detection . . . 152

7.3.9 Ranking 152

7.3.10 Should I make a prediction at all? 153

7.4 Prediction techniques 154

7.4.1 Counting techniques 154

7.4.2 Optimization techniques 160

7.4.3 Other ensembles 162

7.5 Social network analysis 162

7.6 Natural language analytics 171

7.7 Making data analytics available 176

7.8 Demonstrating compliance 177

8 Case studies 181

8.1 Predicting crime rates 181

8.2 Clustering RMS data 184

8.3 Geographical distribution patterns 193

8.4 Risk of gun violence 196

8.5 Copresence networks 199

8.6 Criminal networks with a purpose 204

8.7 Analyzing online posts 206

8.7.1 Detecting abusive language 209

8.7.2 Detecting intent 212

8.7.3 Deception 215

8.7.4 Detecting fraud in text 217

8.7.5 Detecting sellers in dark-web marketplaces 219

8.8 Behavior – detecting fraud from mouse movements 220

8.9 Understanding drug trafficking pathways 221

9 Law enforcement can use interaction too 229

9.1 Structured interaction through transnational organizations . . . 230

9.2 Divisions within countries 232

9.3 Sharing of information about crimes 233

9.4 Sharing of data 233

9.5 Sharing models 235

9.6 International issues 236

10 Summary 239

Bibliography 251

Index 255