

# Contents

<i>Preface</i>	v
1. Terrorism and the Internet: Use and Abuse	1
<i>Abraham R. Wagner</i>	
1.1 Introduction . . . . .	1
1.1.1 Evolution of Cyberspace and the Internet . . . . .	1
1.1.2 A Paradigm Shift and Exponential Growth in Cyberspace . . . . .	5
1.2 Terrorist Use of the Internet . . . . .	7
1.2.1 Terrorist Use of the Internet for Covert Communications	8
1.2.2 Finding Terrorist E-Mail . . . . .	12
1.2.3 The Impact of Encryption . . . . .	13
1.2.4 Non E-mail Techniques . . . . .	16
1.3 Terrorist Access to Information . . . . .	17
1.3.1 Potential Targets for Future Attacks . . . . .	17
1.3.2 Logistics for Terrorist Operations . . . . .	18
1.3.3 Technical Data for Terrorist Operations . . . . .	19
1.4 Terrorist Web Sites . . . . .	20
1.4.1 Platform for Terrorist Propaganda . . . . .	21
1.4.2 Platform for Terrorist Recruitment and Fundraising .	22
1.5 Terrorists and Cyber-Terrorism . . . . .	24
<i>Bibliography</i>	27
2. The Radical Islam and the Cyber Jihad	29

*Shaul Shay*

- 2.1 The New Trends of Terror . . . . . 29
- 2.2 Information Terrorism . . . . . 31
- 2.3 The Cyberspace as Battlefield . . . . . 33
  - 2.3.1 Netwars and Networks . . . . . 33
  - 2.3.2 The Cyberspace as Cyber-Jihad . . . . . 33
  - 2.3.3 The Trends in the Information Age . . . . . 34
- 2.4 Conclusion . . . . . 35

*Bibliography* 39

- 3. Using Data Mining Technology for Terrorist Detection on the Web 41

*Mark Last*

- 3.1 Introduction: Who is Hiding in Cyber Caves? . . . . . 41
- 3.2 Data Mining for Countering Terror in Cyberspace . . . . . 43
  - 3.2.1 Taxonomy of Data Mining Methods . . . . . 43
  - 3.2.2 Data Mining Needs and Challenges for Cyber Security and Cyber Intelligence . . . . . 46
- 3.3 Key Techniques of Cyber Warfare . . . . . 47
  - 3.3.1 Link Analysis . . . . . 47
  - 3.3.2 Information Agents . . . . . 49
  - 3.3.3 Trend Discovery . . . . . 52
  - 3.3.4 Real-Time Data Mining . . . . . 53
  - 3.3.5 Input-Output Analysis of Software Systems . . . . . 56
- 3.4 Summary . . . . . 58

*Bibliography* 59

- 4. A Content-Based Model for Web-Monitoring 63

*Bracha Shapira*

- 4.1 Introduction . . . . . 63
- 4.2 Detailed Description of the Model . . . . . 66
  - 4.2.1 Learning Phase . . . . . 66
  - 4.2.2 The Detection Phase . . . . . 68
- 4.3 Summary . . . . . 69

<i>Bibliography</i>	73
5. TDS — An Innovative Terrorist Detection System	75
<i>Yuval Elovici</i>	
5.1 Introduction . . . . .	75
5.2 Content-Based Methodology for Anomaly Detection: Review	76
5.2.1 Learning the Normal User Behavior . . . . .	77
5.2.2 Detecting Abnormal Users . . . . .	78
5.3 Design Goals . . . . .	79
5.4 TDS Architecture . . . . .	79
5.4.1 On-line HTML Tracer . . . . .	81
5.4.2 Vectorization . . . . .	81
5.4.3 Normal User Behavior Computation . . . . .	82
5.4.4 Detection . . . . .	82
5.5 Performance Measures . . . . .	83
5.6 System Evaluation . . . . .	84
5.7 System Deployment . . . . .	85
5.8 Summary . . . . .	87
<i>Bibliography</i>	89
6. Clustering Algorithms for Variable-Length Vectors and Their Application to Detecting Terrorist Activities	91
<i>Menahem Friedman</i>	
<i>Moti Schneider</i>	
<i>Abraham Kandel</i>	
6.1 Introduction . . . . .	91
6.2 Creating the Centroids . . . . .	94
6.3 Application . . . . .	99
6.3.1 Clustering . . . . .	99
6.3.2 Detection . . . . .	100
6.4 The Experiment . . . . .	100
6.5 Summary . . . . .	101
<i>Bibliography</i>	103

7. Analysis of Financial Intelligence and the Detection of Terror Financing	105
<i>Yehuda Shaffer</i>	
7.1 Introduction . . . . .	105
7.2 Implementation of International Anti Money Laundering Standards in the Combat Against Terror Financing . . . . .	106
7.2.1 The Impact of 9/11 . . . . .	106
7.2.2 Money Laundering and Terror Financing . . . . .	107
7.3 Terror Financing Typologies . . . . .	107
7.3.1 Characteristics of Terror (Not Only Terrorist) Financing . . . . .	107
7.3.2 Why and How Do Terror Groups Launder Money . .	108
7.4 Reporting Duties of Financial Institutions and the Role of Financial Intelligence Units (FIU) in Combating Terror Financing . . . . .	110
7.4.1 A Strategy for Fighting Terror Financing . . . . .	110
7.4.2 Information Received from the Private Sector . . . .	111
7.4.3 The Role of the FIU . . . . .	112
7.4.4 IT Analysis Tools at FIUs . . . . .	113
7.4.5 Terror Financing Investigation . . . . .	114
7.5 Information Available - Possible Future Developments . . .	114
8. Identification of Terrorist Web Sites with Cross-Lingual Classification Tools	117
<i>Alex Markov and Mark Last</i>	
8.1 Introduction . . . . .	117
8.2 Document Categorization and Classification . . . . .	119
8.3 Selected Applications of Web Document Classification . . .	119
8.3.1 Automatic Web News Extraction . . . . .	120
8.3.2 Personalization and E-Commerce . . . . .	121
8.3.3 Organization of Web Document Collections . . . . .	121
8.3.4 Multi-Lingual Applications . . . . .	122
8.4 Document Representation . . . . .	123
8.4.1 Traditional Text Models . . . . .	123
8.4.2 Web Document Models . . . . .	124
8.5 Graph Based Representations of Web Documents . . . . .	125

8.5.1	Graph Structure . . . . .	125
8.5.2	Term Extraction Methods . . . . .	128
8.5.2.1	Naïve Extraction . . . . .	128
8.5.2.2	Smart Extraction . . . . .	128
8.5.3	Frequent Sub-Graph Extraction Problem . . . . .	129
8.6	Cross-Lingual Web Document Classification with Graphs . . . . .	130
8.6.1	Representation and Classification Process . . . . .	130
8.6.2	Web Document Representation Example . . . . .	132
8.7	Case Study: Identification of Terrorist Web Sites in Arabic . . . . .	136
8.7.1	About Document Collection . . . . .	136
8.7.2	Preprocessing of Documents in Arabic . . . . .	137
8.7.3	Experiment and Evaluation of Results . . . . .	138
8.8	Conclusions . . . . .	140
8.9	Acknowledgment . . . . .	141
	<i>Bibliography</i> . . . . .	143
	Appendix A Useful Sources . . . . .	147
	Appendix B Terrorist Web Sites — Examples . . . . .	149
	Appendix C About the Authors . . . . .	157
	<i>Index</i> . . . . .	165