

TABLE OF CONTENTS

Table of Contents vii

Preface xi

Author’s Biography..... xv

Chapter 1. Intelligence and Security Informatics (ISI): Challenges and Opportunities..... 1

Chapter Overview 1

1.1 Introduction..... 3

1.2 Information Technology and National Security 3

1.3 Problems and Challenges 5

1.4 Intelligence and Security Informatics vs. Biomedical Informatics:
Emergence of a Discipline 7

1.5 Federal Initiatives and Funding Opportunities in ISI..... 8

1.6 Future Directions 12

1.7 Questions for Discussion 13

Chapter 2. An ISI Research Framework: Information Sharing and Data Mining..... 15

Chapter Overview 15

2.1 Introduction..... 17

2.2 An ISI Research Framework..... 17

2.3 Caveats for Data Mining 20

2.4 Domestic Security, Civil Liberties, and Knowledge Discovery..... 20

2.5 Future Directions 22

2.6 Questions for Discussion 22

Chapter 3. ISI Research: Literature Review 25

Chapter Overview 25

3.1 Information Sharing and Collaboration 27

3.2 Crime Association Mining 29

3.3 Crime Classification and Clustering 32

3.4 Intelligence Text Mining..... 34

3.5 Crime Spatial and Temporal Mining..... 36

3.6 Criminal Network Analysis 38

3.7 Future Directions 40

3.8 Questions for Discussion 41

Chapter 4. National Security Critical Mission Areas and

Case Studies 43

Chapter Overview 43

4.1 Introduction..... 45

4.2 Intelligence and Warning 45

4.3 Border and Transportation Security 47

4.4 Domestic Counter-terrorism 48

4.5 Protecting Critical Infrastructure and Key Assets..... 49

4.6 Defending Against Catastrophic Terrorism 50

4.7 Emergency Preparedness and Response 51

4.8 Future Directions 53

4.9 Questions for Discussion 53

Chapter 5. Intelligence and Warning 55

Chapter Overview 55

5.1 Case Study 1: Detecting Deceptive Criminal Identities 57

5.2 Case Study 2: The Dark Web Portal 59

5.3 Case Study 3: Jihad on the Web..... 64

5.4 Case Study 4: Analyzing the Al-Qaeda Network..... 67

5.5 Future Directions 72

5.6 Questions for Discussion 73

Chapter 6. Border and Transportation Security 75

Chapter Overview 75

6.1 Case Study 5: Enhancing “BorderSafe” Information Sharing 77

6.2 Case Study 6: Topological Analysis of Cross-Jurisdictional Criminal
Networks 79

6.3 Future Directions 83

6.4 Questions for Discussion 83

Chapter 7. Domestic Counter-terrorism..... 85

Chapter Overview 85

7.1 Case Study 7: COPLINK Detect..... 87

7.2 Case Study 8: Criminal Network Mining..... 90

7.3 Case Study 9: Domestic Extremist Groups on the Web..... 95

7.4 Case Study 10: Topological Analysis of Dark Networks..... 98

7.5 Future Directions 103

7.6 Questions for Discussion 104

Chapter 8. Protecting Critical Infrastructure and Key Assets 105

Chapter Overview 105

8.1 Case Study 11: Identity Tracing in Cyberspace 107

8.2 Case Study 12: Feature Selection for Writeprint 110

8.3 Case Study 13: Developing an Arabic Authorship Model 113

8.4 Future Directions 117

8.5 Questions for Discussion 117

Chapter 9. Defending Against Catastrophic Terrorism..... 119

Chapter Overview 119

9.1 Case Study 14: BioPortal for Disease and Bioagent Surveillance 121

9.2 Case Study 15: Hotspot Analysis and Surveillance 123

9.3 Future Directions 128

9.4 Questions for Discussion 128

Chapter 10. Emergency Preparedness and Response..... 131

Chapter Overview 131

10.1 Case Study 16: Mapping Terrorism Research..... 133

10.2 Case Study 17: A Dialogue System for Terrorism Resources 136

10.3 Future Directions 139

10.4 Questions for Discussion 140

Chapter 11. The Partnership and Collaboration Framework..... 141

Chapter Overview 141

11.1 Introduction..... 143

11.2 Ensuring Data Security and Confidentiality..... 143

11.3 Reaching Agreements among Partners 144

11.4 The COPLINK Chronicle 148

11.5 Future Directions 150

11.6 Questions for Discussion 151

Chapter 12. Conclusions and Future Directions 153

Chapter 13. Acknowledgements 157

Chapter 14. References..... 161

Subject Index..... 173