

PREFACE

Terrorism informatics is defined as the application of advanced methodologies and information fusion and analysis techniques to acquire, integrate, process, analyze, and manage the diversity of terrorism-related information for national/international and homeland security-related applications. These techniques are derived from disciplines such as computer science, informatics, statistics, mathematics, linguistics, social sciences, and public policy. Because the study of terrorism involves copious amounts of information from multiple sources, data types, and languages, information fusion and analysis techniques such as data mining, data integration, language translation technologies, and image and video processing are playing key roles in the future prevention, detection, and remediation of terrorism¹. Within the homeland security industry, information fusion is defined as the use of computer technology to acquire data from many sources, integrate this data into usable and accessible forms, and interpret the results². Although there has been substantial investment and research in the application of computer technology to terrorism, much of the literature in this emerging area is fragmented and often narrowly focused within specific domains such as engineering, computer science, computer security, information systems, knowledge management, and biomedicine.

The goal of this edited volume is to present an interdisciplinary and understandable review of terrorism informatics work for homeland security along two dimensions: methodological issues in terrorism research, including information infusion techniques to support terrorism prevention, detection, and response; and legal, social, privacy, and data confidentiality challenges and approaches.

SCOPE AND ORGANIZATION

This book has been grouped into two units. Unit I focuses on the methodological issues in terrorism research including trends, achievements and failures in terrorism research, methodological challenges in terrorism, challenges in retrieving and sharing terrorism information resources, and root causes of terrorism and the implications for terrorism informatics. It

¹ National Research Council, 2003. Making the Nation Safer: the Roles of Science and Technology in Countering Terrorism, p11.

² Ibid, p. 166.

also attends to critical socio-technical topics relevant to information and knowledge management such as privacy, data confidentiality, and legal challenges. Unit I chapters address the following topics and concepts:

- Mapping the domain of terrorism research
- Identifying key terrorism researchers
- The impact on 9/11 on terrorism
- Primary sources for the study of terrorism
- Analyzing the root causes of terrorism
- The construction of information resources useful for the study of terrorism
- Threat assessment and analysis
- Methods to support counterterrorism
- Data mining and privacy concerns

Unit 2 presents current research, including case studies, on the application of terrorism informatics techniques (such as web mining, social network analysis, and multimodal event extraction and analysis) to the terrorism phenomenon. Unit 2 focuses on three major areas of terrorism research: prevention, detection, and response as identified by the National Research Council³ and the U.S. White House's Office of Science and Technology Program (OSTP).⁴ Unit III will present the critical sociotechnical topics relevant to information and knowledge management: social, privacy, data confidentiality, and legal challenges.

- Examining "Jihad" on the world wide web
- Comparing extremist groups websites across regions
- Analyzing extremist communications as manifested in web forums
- Terrorist analysis systems and detection
- Identification of potential bioterrorist weapons
- Detecting and analyzing anomalous content
- Examining "insider" threats
- Using web mining and social network analysis
- Video analysis and deception detection
- Situational awareness technologies for disaster response

³ Ibid., p. 167.

⁴ Zahn, M.A. and Strom, K.J., 2004, "Terrorism and the Federal Social Science Research Agenda". Edited by M. DeFlem. In *Terrorism and Counter-Terrorism: Criminological Perspectives*. Elsevier p112.

CHAPTER STRUCTURE

Each chapter follows a consistent structure to ensure uniformity and ease of use:

- Title
- Authors and affiliations
- Introduction: introduces the relevance and significance of the topic
- Literature review/Overview of the field: a systematic review of related works in the topic area
- Case study/Methods/Examples: One or two detailed studies or examples of selected techniques, systems, implementations and evaluations
- Conclusion and discussion
- Acknowledgements
- References and notes
- Suggested readings
- Online resources
- Questions for discussion

The work is further enhanced by author and subject indexes at the back of the book, intended to facilitate ease of access to the contents./

INTENDED AUDIENCE

The audience of the book is intentionally broad. It is intended to bring useful knowledge to scientists, security professionals, counterterrorism experts, and policy makers. It is also intended to serve as reference material and as a textbook in graduate-level courses related to information security, information policy, information assurance, information systems, terrorism, and public policy. Readers will learn new concepts, technologies, and practices developed in terrorism informatics through the comprehensive reviews of recent work and detailed case studies presented in each chapter. Students and researchers will broaden their understanding and knowledge in these new research topics. Practitioners will be able to better evaluate and/or employ new and alternative technologies for their current projects and future work.

Terrorism Informatics

Knowledge Management and Data Mining for Homeland
Security

Chen, H.; Reid, E.; Sinai, J.; Silke, A.; Ganor, B. (Eds.)

2008, XLII, 558 p., Hardcover

ISBN: 978-0-387-71612-1