Review of the book

"Terrorism Informatics"
by Hsinchun Chen, Edna Reid, Joshua Sinai, Andrew Silke, Boaz Ganor
Springer, 2009

ISBN-13: 978-0-387-71612-1

Olivier Blazy, ENS/CNRS/INRIA, France

2010-01-08

1 What the book is about

This book is a compilation of the actual state of research in the field of Terrorism Informatics, which is defined as the use of advanced techniques to acquire, process and analyses a vast amount of terrorism-related information for security application. After a small preface, about the book organization and short biographies of the different authors, the book is divided into two main units :

- The first one (nearly a third of the book) is entitled *Methodological Issues in Terrorism research.* Through ten chapters we'll be explained different approaches of the terrorism research problem, from Group Learning Patterns to Databases, by trying to determine the root causes, the key figures in terrorism studies.

  In Chapter 1 (Domain Mapping of Contemporary Terrorism Research), we are given an overview of contemporary terrorism research thanks to visualization techniques on data from the last 40 years. It shows 42 main terrorism researchers, their influential results, ...

  In Chapter 2 (Research on Terrorism: A review of the impact of 9/11 and the Global War on Terrorism), the paper highlights the increase of interest in terms on publications on terrorism topics since 9/11, and shows that it can improve the quality of the conclusions being reached.

  In Chapter 3 (Who are the Key Figures in "Terrorism Studies"), we are presented a framework useful to determine the key figures in terrorism studies, to provide effective foundations to research in this field. The next part tries to categorize key researchers in three pools according to their number of publications.

  In Chapter 4 (Interviewing Terrorists: A Case for Primary Research), we are explained that field research may be more valuable than often considered and may help researchers on terrorism not to be misinformed.

  In Chapter 5 (Resolving a Terrorism Insurgency by Addressing its Root Causes), explains the importance of mapping root causes in a conflict, as it is one of the initial components in the terrorism life cycle.

  In Chapter 6 (A quantitative analysis of "Root Causes of Conflict"), we are presented methods of measurements based on Latent Semantic Analysis, a statistical analysis on semantic similarity across a corpus of documents, and its application to a wide corpus.

  In Chapter 7 (Countering Terrorism with Knowledge), we are explained that sharing knowledge is required to fight terrorism, and explains why the Memorial Institute for the Prevention of Terrorism shares many information, even its Terrorism Knowledge base.

In Chapter 8 (Toward a Target-Specific Method of Threat Assessment), we discover a model used at the Institute for Counter-Terrorism, used to detect potential target and find credible attack scenarios.

In Chapter 9 (Identifying and Exploiting Group Learning Patterns for Counterterrorism), we are presented a model of organizational learning and shown how it can be used for data analysis efforts.

Chapter 10 (Homeland Insecurity) deals with the problems of matching information through different databases, it also explains worries about confidentiality and introduce the concept of ”selective revelation”.

- In the second unit, the editors have compiled fourteen papers on *Terrorism Informatics to support prevention, detection and response.* In those chapters we are presented different notions, like a web mining approach, data distortion methods, text mining, and social networks analysis.

  In Chapter 11 (Case Study of Jihad on the Web), we are shown some procedures of (semi-)automated procedures and methodologies to capture terrorist Website data and construct a terrorist social network.

  In Chapter 12 (Studying Global Extremist organizations' Internet Presence Using the Darb Web Attribute System), shows an application of automated web crawling to build a database, they used to study from three perspectives: technical sophistication, content richness, Web interactivity. They conclude by saying that all studied organization showed a high level of technical level.

  In Chapter 13 (Content Analysis of Jihadi Extremist Groups' Video), we see how they try to automatize the analysis of videos posted on a terrorist website in order to find effective countermeasures.

  In Chapter 14 (Analysis of Affect Intensities in Extremist Group Forums), they focus on group forums and show how they detect hate and violence in several posts with a probabilistic disambiguation technique. Their results shows that Middle Eastern groups are more violent than US ones, and that the more a group is hateful on his website, the more violent it is.

  In Chapter 15 (Document Selection for Extracting Entity and Relationship Instances of Terrorist Events), we have the result of a study on an automated Information Extraction task who find relevent information on relation instances from documents and then sort them through different ranking strategies. They conducted two experiments on historical terrorism events and showed that their methodology works well.

  Chapter 16 (Data Distorsion Methods and Metrics in a Terrorist Analysis System) introduced a Singular Value decomposition method for data distorsion which helps maintain privacy without decreasing the utility of datasets it is applied on.

  Chapter 17 (Content-Based Detection of Terrorists Browsing the Web Using an Advanced Terror Detection System), introduced an improvement of the actual Terrorist Detection System (TDS). This improvement aims at decreasing the number of false positive.

  Chapter 18 (Text Mining the Biomedical Literature for Identification of Potential Virus/Bacterium as Bio-terrorism Weapons), has as self-explanatory title. The presented result is intended to lead to appropriate defense and/or public health measure.

  Chapter 19 (Leveraging One-Class SVM and Semantic Analysis to Detect Anomalous Content), introduced a Semantic Anomaly Monitor system which outperforms both Natural Language Processing and Bag-of-Words in precision, recall and performance.

  Chapter 20 (Individual and Collective Analysis of Anomalies in Message Traffic) presents a two-pronged approach to detect abnormal behavior, first you use a standard approach, and you focus on people reaction, those who change their behavior knowing they are monitored have higher chance to be detected as suspects.

  Chapter 21 (Addressing Insider threat Through Cost-Sensitive Document Classification), presents a framework in compliance with a ”need to know” security, which is cost-sensitive and tries to avoid false positive (access for an unauthorized user) more than false negative (denial for an authorized user).

Chapter 22 (Using Web Mining and Social Network Analysis to Study the Emergence of Cyber Communities in Blogs), presents a framework analyzing blogs. they studied 28 anti-Blacks groups and distinguished 2 different main communities among them. The authors think the framework can be applied to other domains.

Chapter 23 (Automatic Extraction of Deceptive Behavioral Cues from Video), presents a study on how to analyze expression on videos to detect indicator of deception.

Chapter 24 (Situational Awareness Technologies for Disaster Response), is about the RESCUE project and particularly the situational awareness technologies. After presenting the different outcomes of the project they also provide an overview of transition activities.

2 What the book is like

The editors tried to organize their book along two dimensions. First they group a selection of papers on methodological issues in terrorism research; with papers quite global on the area, whereas in the second unit they go into the detail with specific examples on how to deal with suspicious information. Each chapter follows the same structure, after the standard information (title and the authors' names) you can find a brief introduction to the topic on which the chapter is about where the author tries to explain why their development is relevant and useful. Then you have a short overview of the field, in order to introduce the case study they want to speak about, with some examples. After the conclusion, you can find some references, links to on-line resources and some questions.

I like the brief overview at the beginning of each paper, it helps to understand the problems, needs of each topic, even if you are not really used to the field. The final questions at the end of each chapter are also interesting, they help to understand what has just been presented, and also might give ideas, guidelines to motivate further work, which can be quite useful. Most of the scheme and frameworks presented are immediately applied to concrete examples or databases, so the reader may understand easily how it works, and what is the expected outcome.

3 Recommendation

It's never easy to determine who is the best target for a given book. The different papers cover a wide range of the field, so I believe everyone can find something new in this book. The chapter overviews, and the ending questions might be more useful for a student, neophyte in the field, helping him understand what is at stake and why a specific approach is relevant. However as most of the papers contain specific tables and figures on actual real examples, I believe that even specialists can find useful information in the book. And as I said before, the ending questions might give guidelines to further studies in the field.

From the reviewer's point of view there is however a minor drawback. If we exclude the preface, the book is just a compilation of papers on *Terrorism Informatics.* One might have expected some cohesion between them, to see a kind of progression throughout the book, whereas here you take a glimpse to many different areas but without any link between them, at least nothing more than they all gravitate around terrorism informatics. On the same idea a conclusion at the end of each unit might have been a good idea to summarize the key elements presented.

Nevertheless, the audience is still really broad. As I said, on the one hand, specialists (scientific, experts, policy makers) can find useful information, on the other hand, the book is really accessible to students. The book might help to learn new concepts, technologies, and also to find new alternative approaches to existing problems, and gives a good review of current state of the are in the Terrorism Informatics field.

The reviewer is a Ph.D. student at the Ecole Normale Supérieure, Paris, France.