

Chapter 19

Conceptual Tools for Dealing with ‘Narrative’ Terrorism Information

Gian Piero Zarri
University Paris-Est, France

ABSTRACT

In this paper, we evoke first the ubiquity and the importance of the so-called ‘non-fictional narrative’ information, with a particular emphasis on the terrorism- and crime-related data. We show that the usual knowledge representation and ‘ontological’ techniques have difficulties in finding complete solutions for representing and using this type of information. We supply then some details about NKRL, a representation and inferencing environment especially created for an ‘intelligent’ exploitation of narrative information. This description will be integrated with concrete examples to illustrate the use of this conceptual tool in a terrorism context.

INTRODUCTION

‘Narrative’ information concerns the account of some real-life or fictional story (a ‘narrative’) involving concrete or imaginary ‘personages’. In this paper, we will deal with those (*multimedia*) *non-fictional narratives* that are typically embodied into corporate memory documents (memos, policy statements, reports, minutes, documentation archives for product development...), news stories, normative and legal texts, medical (or financial, cadastral, administrative...) records, audit reports, many intelligence messages, surveillance videos or visitor logs, actuality photos and video fragments for newspapers and magazines, eLearning and Cultural Heritage material (text, image, video, sound...), plotting and narrative course of actions for videogames, etc.

Note, in particular, that dealing with non-fictional narrative material is of paramount importance for analysis and management of any sort of *crisis situation* and, more in general, *for enhancing the ability*

DOI: 10.4018/978-1-60566-836-9.ch019

to fight terrorism and other crimes. For example, six critical mission areas have been identified in the “National Strategy for Homeland Security” report (2002). Of these, at least two, “Intelligence and Warning” and “Domestic Counter-terrorism” are based on the processing of non-fictional narrative information in order, e.g., to “... find cooperative relationships between criminals and their interactive patterns”. Managing non-fictional narrative information must then be considered as an essential component of the emerging science of “Intelligence and Security Informatics” (ISI), as defined, e.g., in (Chen and Wang, 2005; Chen, 2006).

From a concrete point of view, ‘non-fictional narratives’ deal with *the description of spatially and temporally characterized ‘events’* that relate, at some level of abstraction, the behavior or the state of given real-life ‘actors’ (characters, personages, etc.): these try to attain a specific result, experience particular situations, manipulate some (concrete or abstract) materials, send or receive messages, buy, sell, deliver etc. Note that:

- The term ‘event’ is taken here in its *most general meaning*, covering also strictly related notions like fact, action, state, situation, episode, activity etc.
- The ‘actors’ or ‘personages’ involved in the events *are not necessarily human beings*: we can have narratives concerning, e.g., the vicissitudes in the journey of a nuclear submarine (the ‘actor’, ‘subject’ or ‘personage’), the various avatars in the life of a commercial product, or the description of an industrial equipment that passes from an ‘idle’ to a ‘working’ state.
- Even if a large amount of non-fictional narratives are embodied within natural language (NL) texts, this is *not necessarily true*: narrative information is really ‘*multimedia*’. A photo representing a situation that, verbalized, could be expressed as “The US President is addressing the Congress” is not of course an NL document, yet it surely represents a narrative.

In this paper, we will present an Artificial Intelligence tool, NKRL, “Narrative Knowledge Representation Language”, see (Zarri, 2003; 2005a; 2009) that is, at the same time:

- a *knowledge representation system* for describing in some detail the essential content (the ‘meaning’) of complex non-fictional narratives;
- a system of *reasoning (inference) procedures* that, thanks to the richness of the representation system, is able to automatically establish ‘interesting’ relationships among the represented data;
- an *implemented software environment*.

The paper will be illustrated mainly by examples concerning a successful application of NKRL techniques on the news stories inserted in a “Southern Philippines terrorism” corpus used in an R&D European project, see (Zarri, 2005a). The success of this application has confirmed that it could be possible to make use of NKRL as a useful and powerful investigation tool to be employed in any sort of ‘defense’ and ‘crisis management’ applications. Another successful, exploratory study concerning the use of NKRL to detect specific crisis situations through an in-depth conceptual analysis of news stories about Afghanistan has been also recently carried out in collaboration with the French “*Délégation Générale pour l’Armement*” (DGA, Central Bureau for Armaments); some information (and an example) on this last experiment will also be supplied in the following Sections.

21 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage:

[www.igi-global.com/chapter/conceptual-tools-dealing-narrative-
terrorism/39229](http://www.igi-global.com/chapter/conceptual-tools-dealing-narrative-terrorism/39229)

Related Content

Reversible Watermarking in Medical Image Using RDWT and Sub-Sample

Lin Gao, Tiegang Gao and Jie Zhao (2015). *International Journal of Digital Crime and Forensics* (pp. 1-18).
www.irma-international.org/article/reversible-watermarking-in-medical-image-using-rdwt-and-sub-sample/139231

Challenges to Digital Forensic Evidence in the Cloud

Fred Cohen (2013). *Cybercrime and Cloud Forensics: Applications for Investigation Processes* (pp. 59-78).
www.irma-international.org/chapter/challenges-digital-forensic-evidence-cloud/73958

Identifying the Use of Anonymising Proxies to Conceal Source IP Addresses

Shane Miller, Kevin Curran and Tom Lunney (2021). *International Journal of Digital Crime and Forensics* (pp. 1-20).
www.irma-international.org/article/identifying-the-use-of-anonymising-proxies-to-conceal-source-ip-addresses/279371

Answering the New Realities of Stalking

Avelina Alonso de Escamilla (2015). *Handbook of Research on Digital Crime, Cyberspace Security, and Information Assurance* (pp. 67-76).
www.irma-international.org/chapter/answering-the-new-realities-of-stalking/115749

LUARM: An Audit Engine for Insider Misuse Detection

G. Magklaras, S. Furnell and M. Papadaki (2011). *International Journal of Digital Crime and Forensics* (pp. 37-49).
www.irma-international.org/article/luarm-audit-engine-insider-misuse/58407