

# Cyberinfrastructure for homeland security: Advances in information sharing, data mining, and collaboration systems

T.S. Raghu<sup>a,\*</sup>, Hsinchun Chen<sup>b,1</sup>

<sup>a</sup> BA301G, W. P. Carey School of Business, Department of Information Systems, BOX No. 874606, Arizona State University, Tempe, AZ 85287, United States

<sup>b</sup> Management Information Systems Department, MCCL 430Z, The University of Arizona, Tucson, AZ 85721, United States

Available online 11 May 2006

## 1. Introduction

Most disaster scenarios faced by agencies entrusted with homeland security require timely access to relevant information that can be sensed and acted upon. However, the required data and information often reside in silos that are isolated from each other due to jurisdictional boundaries or representational incompatibilities. Given the nature of the threat to homeland security, regional, cross-institutional data sharing is a necessary first step towards effective crisis response measures. The purpose of this special issue is to encourage research discussions of practical and novel cyberinfrastructure technologies, techniques, methods, practices, and systems that can contribute to knowledge in this important emerging area. The intent was to publish relevant work that contribute to the application of state-of-the-art knowledge of information sharing, data mining or collaboration systems to the context of homeland security.

The 2003 NSF Workshop on “Cyberinfrastructure Research for Homeland Security” defined Cyberinfrastructure as a key technology enabler that facilitates the federation of distributed information and knowledge resources to reduce constraints of distance and time. Cy-

berinfrastructure systems have gradually evolved over the last three decades. However, in the wake of the security needs since September 11, 2001, existing approaches to information sharing, data mining and collaboration need to be re-examined and adapted for national security applications. The Call for Papers for this special issue closely followed the recommendations of the workshop and invited contributions from a number of topic areas such as event detection and surveillance, intrusion and deception detection, collaborative decision-making, intelligent agent support, and visualization and situational awareness.

## 2. In this issue

We received over 20 submissions that were put through a rigorous review process involving over 50 reviewers in the field. The review process resulted in the acceptance of 8 quality papers for the special issue. The papers include a very good cross-section of current research on Cyberinfrastructure for security. The included papers make very important contributions to Cyberinfrastructure research stream by focusing on the development of novel techniques and tools for information analysis, pattern discovery, data warehousing and information retrieval. One of the papers explores issues related to citizens’ interaction with Cyberinfrastructure resources, especially when the security environment is experiencing turbulence.

The lead paper by Carley et al. (“Toward an interoperable dynamic network analysis toolkit”), discusses a

\* Corresponding author. Tel.: +1 480 965 8977; fax: +1 480 965 8392.

E-mail addresses: [Raghu.Santanam@asu.edu](mailto:Raghu.Santanam@asu.edu) (T.S. Raghu), [hchen@eller.arizona.edu](mailto:hchen@eller.arizona.edu) (H. Chen).

URLs: <http://wpcarey.asu.edu/Directory/stafffaculty.cfm?cobid=1039602&from=dept> (T.S. Raghu), <http://ai.arizona.edu/hchen> (H. Chen).

<sup>1</sup> Tel.: +1 520 621 2748; fax: +1 520 621 2433.

dynamic network analysis toolkit to facilitate analysis and visualization of complex socio-technical systems. The paper lays out the requirements for a software tool-chain design that includes extensibility, interoperability, common ontological framework and interchange language, scalability and robustness. The resulting toolkit addresses the requirements by incorporating existing tools as well as building new ones. The potential usefulness of the toolkit is demonstrated through an illustrative example.

In the second paper (“An Associate constraint network approach to extract multi-lingual information for crime analysis”), Yang and Wing Li pose an interesting problem in international crime and terrorism scenario. Most communication and relevant records in a global context would not be in a single language, therefore necessitating “cross-lingual semantic interoperability.” The authors improve upon their Hopfield network approach to cross-lingual concept space generation using a constraint satisfaction problem formulation. Using English/Chinese press releases of the Hong Kong police, the performance capabilities of the Associate constraint network approach are investigated.

The third paper (“Genetic programming for prevention of cyberterrorism through dynamic and evolving intrusion detection”), by Hansen et al., motivates a self-correcting and self-maintaining approach to computer security. The authors propose a genetic programming approach as an adaptive mechanism for real-time intrusion detection. The encouraging results from the method’s application to a large dataset sourced from DARPA and Lincoln laboratories at MIT prompts one to investigate and develop effective learning systems as the foundation for designing intrusion detection mechanisms.

The next two papers tackle novel information discovery and storage mechanisms tailored to intelligence and counterterrorism needs. In the paper — “Novel information discovery for intelligence and counterterrorism” — Skillicorn and Vats present the design of a discovery procedure that returns contextualized information that cannot easily be discovered. The procedure ensures that the search process does not get unnecessarily skewed by the choice of search keywords and acquires new information in the context of central concepts embodied by the keywords. The utility of the system is demonstrated by executing the system as if on September 12, 2001. The next paper — “The role of data warehousing in Bioterrorism surveillance” — by Berndt et al., explores the role of data warehousing in surveillance systems. The authors present data warehousing as a complementary technology to syndromic systems. While surveillance using a historical data warehouse alone is “infeasible,” techniques described in this paper are invaluable in an integrated bioterrorism surveillance architecture. The authors use the Florida wildfires data from 1996 to

2001 in interesting ways to demonstrate the usefulness of OLAP techniques in this context.

Relevance is key to reducing cognitive load on intelligence analysts in their search for potentially harmful information. The role of Question Answering (QA) technology in enhancing relevance of search and retrieval is the topic of interest in two papers. Both papers take an experimental approach to investigate the effectiveness of QA technology. The paper by Roussinov and Robles-Flores (“Applying question answering technology to locating malevolent online content”) compares keyword searching to QA technique on the capability of locating potentially malevolent online content. The authors establish through a human–computer interaction study that QA tools can potentially enhance the relevance of returned searches and hence allow for automating such searches at intelligence agencies, where trends and changes in retrieved results on a daily basis can be tracked and analyzed. The second paper on QA technique — “Leveraging question answering technology to address terrorism inquiry” — by Schumaker and Chen investigates the use of a QA system in the dissemination of terrorism information to the general public. The results from their experiments indicate that a conversational tone to knowledge bases might be a better approach when compared to a definitional tone. Both the papers point to the need for more investigations into innovative system design for enhancing the effectiveness of information retrieval and dissemination abilities from large text based information sources.

The final paper (“Perceived risks, counter-beliefs and intentions to use anti-counter-terrorism websites”) by Lee and Rao aptly addresses the need for system designers to consider user perceptions when building counterterrorism related information systems. As the authors point out, the citizens are increasingly dependent on the Internet for government information and services. The unique aspect of the research is the timing of the two surveys conducted as part of the study: the first survey was conducted when the threat level was Orange and the second survey was conducted when the threat level was at a lower yellow level. Interestingly, perceived risk of terrorist attack does not necessarily increase citizen’s intention to use counterterrorism systems significantly. Essentially, citizen’s and government agencies may think differently about the perceived threats.

### 3. Summary

In summary, the special issue papers address very interesting and relevant issues related to Cyberinfrastructure for homeland security. It has been a privilege to guest edit this issue and be involved in the intellectual endeavors of

researchers at the fore front of these efforts. We especially thank Professor Andrew Whinston, Editor-in-chief of Decision Support Systems, for giving us this opportunity and thank all the reviewers for their diligent effort in ensuring the quality of the papers. We thank all the authors for contributing their work to the special issue and bearing with us on some delays in the review process. We hope the readers share our enthusiasm for the papers published in this issue and for their relevance in advancing novel innovations in information systems specifically targeted to counterterrorism efforts.



T.S. Raghu is the Associate Professor of Information Systems in Arizona State University and Director of Research of the Technology Research Center (CABIT). He received his PhD in Management Information Systems from SUNY Buffalo in 1999. His research interests are in Business Process Change, Knowledge Management and Collaborative Decision Making. He has also worked as a systems consultant at leading international IT consulting firms. His publications have appeared in refereed international

journals such as *Information Systems Research*, *Management Science*, *Journal of Organizational Computing and Electronic Commerce*, *Decision Support Systems* and *Expert Systems with Applications*. A number of his papers have also appeared in the proceedings of refereed international conferences such as ICIS, AIS, and Informis.



Dr. Hsinchun Chen is a McClelland Professor of Management Information Systems at the University of Arizona and Andersen Consulting Professor of the Year (1999). He received the BS degree from the National Chiao-Tung University in Taiwan, the MBA degree from SUNY Buffalo, and the PhD degree in Information Systems from the New York University. He is the author/editor of 10 books and more than 130 SCI journal articles covering intelligence analysis, biomedical informatics, data/text/web mining, digital library, knowledge management, and Web computing. He serves on the editorial board of *ACM Transactions on Information Systems*, *IEEE Transactions on Intelligent Transportation Systems*, *IEEE Transactions on Systems, Man, and Cybernetics*, *Journal of the American Society for Information Science and Technology*, and *Decision Support Systems*.