



ELSEVIER

Available online at www.sciencedirect.com

SCIENCE @ DIRECT®

Decision Support Systems 41 (2006) 555–559

Decision Support
Systems

www.elsevier.com/locate/dsw

Editorial

Intelligence and security informatics: information systems perspective

1. Making the nation safer: the role of science and technology

The scientific, engineering, and health communities are increasingly committed to helping the U.S. and the world respond to security challenges after September 11, 2001. The U.S. National Research Council's report on "Making the Nation Safer: The Role of Science and Technology in Countering Terrorism" [3] explains the context of such a commitment:

Terrorism is a serious threat to the security of the United States and indeed the world. The vulnerability of societies to terrorist attacks results in part from the proliferation of chemical, biological, and nuclear weapons of mass destruction, but it also is a consequence of the highly efficient and interconnected systems that we rely on for key services such as transportation, information, energy, and health care. The efficient functioning of these systems reflects great technological achievements of the past century, but interconnectedness within and across systems also means that infrastructures are vulnerable to local disruptions, which could lead to widespread or catastrophic failures. As terrorists seek to exploit these vulnerabilities, it is fitting that we harness the nation's exceptional scientific and technological capabilities to counter terrorist threats.

Leading scientific, engineering, medical, and policy experts in the U.S. conducted the study described in the report. Eight panels were separately appointed in critical national and homeland security research areas including: (1) biological sciences, (2) chemical

issues, (3) nuclear and radiological issues, (4) information technology, (5) transportation, (6) energy facilities, cities, and fixed infrastructure, (7) behavioral, social, and institutional issues, and (8) systems analysis and systems engineering. The focus of the panels' work was on making the nation safer from emerging terrorist threats that would seek to inflict catastrophic damage on the nation's people, its infrastructure, or its economy.

The chapter on information technology (IT) is particularly relevant to this special issue. The report recommends that "a strategic long-term research and development agenda should be established to address three primary counter-terrorism-related areas in IT: information and network security, the IT needs of emergency responders, and information fusion and management." The R&D in information and network security should include approaches and architectures for prevention, identification, and containment of cyber-intrusions and recovery from them. The R&D to address IT needs of emergency responders should include ensuring interoperability, maintaining and expanding communications capability during an emergency, communicating with the public during an emergency, and providing support for decision makers. The R&D in information fusion and management for the intelligence, law enforcement, and emergency response communities should include data mining, data integration, language technologies, and processing of image and audio data. Much of the research reported in this special issue is related to information fusion and management for homeland security.

2. National strategy for homeland security: roles of IT researchers

Since September 11, 2001, the U.S. has taken great strides to improve security. Citizens, industry, academic, and government leaders from across the political spectrum have cooperated to a degree rarely seen in American history. In the first report issued by the Office of Homeland Security in July 2002 [4], several critical mission areas and foundations for an effective national strategy have been identified.

The National Strategy for Homeland Security report aligns and focuses homeland security functions into six critical mission areas, which would benefit significantly from emerging IT research:

- **Intelligence and Gathering:** IT researchers can help build new intelligence gathering and analysis capabilities for an intelligence and warning system that can detect future terrorist activities.
- **Border and Transportation Security:** IT researchers can help develop identity management and deception detection techniques for creating “smart borders”.
- **Domestic Counter-terrorism:** IT researchers can improve information sharing and crime analysis abilities of local, state, and federal crime fighters.
- **Protecting Critical Infrastructure and Key Assets:** IT researchers can help develop the best analytic, modeling, and simulation tools for critical infrastructure and cyberspace protection.
- **Defending against Catastrophic Threats:** IT researchers can help develop simulation, detection, and alerting techniques for potential chemical and biological attacks.
- **Emergency Preparedness and Response:** IT researchers can help improve information sharing and communication interoperability for the first responders before and during emergencies.

The National Strategy for Homeland Security report also describes four foundations—unique American strengths that cut across all of the mission areas, across all levels of government, and across all sectors of our societies. These foundations are Law, Science and Technology, Information Sharing and Systems, and International Collaboration. As a model democratic society, the U.S. has relied on

laws to promote and safeguard its security and liberty. After September 11, new laws and policies to facilitate inter-agency and international information sharing and collaboration have continued to develop and evolve. It is agreed that Science and Technology and Information Sharing and Systems are the two major technical advantages that U.S. possesses to counter terrorism. Many short-term, mid-term, and long-term IT research and development efforts for national and homeland security are critically needed.

3. Developing the science of “Intelligence and Security Informatics” (ISI)

As one of the original founding mandates of the National Science Foundation in the U.S., mid-to-long-term national security research in the areas of information technologies, organizational studies, and security-related public policy is critically needed. Similarly to medical and biological research, law enforcement, criminal analysis, and intelligence communities face significant information overload and yet also have tremendous opportunities for innovation. We believe that, as in “medical informatics” and “bioinformatics”, there is a pressing need to develop the science of “intelligence and security informatics”—the study of the use and development of advanced information technologies, systems, algorithms, and databases for national security related applications through an integrated technological, organizational, and policy based approach.

Many existing computer and information systems techniques need to be reexamined and adapted for national security applications. New insights from this unique domain could result in significant breakthroughs in data mining, visualization, knowledge management, and information security techniques and systems. For example, social network analysis technologies and methodologies could be adopted to help the intelligence community detect planned future attacks, and uncover and understand Bin Laden’s terrorist networks. Visual data mining techniques such as association rules and multidimensional information visualization could be used to identify criminal relationships. Record linkage and string comparator algorithms could be useful for criminal identity deception detection.

Practical and novel information technologies, techniques, methods, practices, and systems that can contribute to knowledge in this important emerging field are critically needed, including but not limited to areas such as:

- Information interoperability and sharing
- Knowledge discovery and knowledge management
- Criminal data mining, social network analysis, and event detection
- Multimedia and multilingual intelligence and security information analysis
- Web-based intelligence monitoring and analysis
- Deception detection systems
- Intrusion detection systems and information awareness
- Cybercrime detection and analysis
- Agents and collaborative systems for intelligence sharing
- Crime and intelligence visualization
- Bio-terrorism tracking, alerting, and analysis
- Major (natural and man-made) disaster prevention, detection, and management

Academic meetings have begun to emerge to encourage research and discussions in ISI-related areas. The First Symposium on Intelligence and Security Informatics (ISI 2003, <http://ecom.arizona.edu/ISI>), sponsored by NSF and NIJ, is such an example. It aimed to provide an intellectual forum for discussions among previously disparate communities: academic researchers (in information technologies, computer science, public policy, and social studies); local, state, and federal law enforcement and intelligence experts; and information technology consultants and practitioners, at a time when several federal research programs, such as the NSF/CIA funded Knowledge Discovery and Dissemination (KDD) program and the NSF Information Technology Research (ITR) program, were seeking new research ideas and projects that could contribute to national security.

Jointly hosted by the University of Arizona and the Tucson Police Department, the NSF/NIJ ISI Symposium program committee was composed of 44 internationally renowned researchers and practitioners in intelligence and security informatics research. The 2-day program included 5 keynote speakers, 14 invited speakers, 34 regular papers, and 6 posters. The

proceedings were published by Springer-Verlag as Lecture Notes in Computer Science (LNCS 2665) [1].

With overwhelming interest and support from the community, the Second ISI Symposium was held in Tucson on June 10–11, 2004 [2]. Sponsoring federal agencies included NSF, DHS, CIA, and NIJ. Jointly hosted by the University of Arizona, Tucson Police Department, and the San Diego Supercomputer Center, the meeting was co-located with the ACM/IEEE Joint Conference on Digital Libraries (JCDL 2004, <http://www.jcdl2004.org>). It is our belief that meetings such as the ISI Symposium and publications such as this special issue on ISI are critical in helping to develop the science of Intelligence and Security Informatics.

4. In this issue

This special issue consists of eight papers that report research in Intelligence and Security Informatics. Most research developed or adopted advanced information systems technologies for national and homeland security applications. The techniques and methodologies reported in the special issue include: discrete choice theory, principal clusters analysis, genetic algorithm, outlier-based data association method, workflow modeling, agent-based decision-making, agent-based simulation model, and data mining. The intelligence and security applications reported include criminal incidents analysis, web community and intelligence mining, information security investment decision support, law enforcement workflow and collaboration, team-based intelligence sharing, diseases and biological attacks simulation, and cybercrime research.

The first paper, “Spatial Analysis with Preference Specification of Latent Decision Makers for Criminal Event” by Xue and Brown, describes a project that combines recent advances in discrete choice theory and data mining to develop point process model for spatial analysis. The methodology was used to analyze and predict the spatial behavior model of criminals. Their evaluation showed that two proposed spatial choice models outperformed the traditional hot spot model. The second paper, “Mining Web Navigations for Intelligence” by Wu, Gordon, DeMaagd, and Fan, presents the principal clusters analysis approach for analyzing user navigations on the Web. The technique

identifies prominent navigation clusters on different user topics based on millions of user navigations. In their experiment, they were able to identify principal cluster such as "crime tutorials" that includes top hub and authority such as "anarchist' cookbook" and "making plastic explosives". The third paper, "Matching Information Security Vulnerabilities to Organizational Security Profiles: A Genetic Algorithm Approach" by Gupta, Rees, Chaturvedi, and Chi, presents and evaluates a genetic algorithm-based approach to enable organizations to choose the minimal-cost security profile providing the maximal vulnerability coverage. The approach provides favorable results in comparison to an enumerative approach in a set of simulated vulnerability scenarios. The fourth paper, "An Outlier-based Data Association Method for Linking Criminal Incidents" by Lin and Brown, presents a new outlier-based approach to resolving the criminal association problem. Using a robbery dataset from Richmond, VA, their experiments showed that the proposed outlier-based model was more effective than a benchmark similarity-based association model. The fifth paper, "Process-Driven Collaboration Support for Intra-Agency Crime Analysis" by Zhao, Bi, Chen, and Zeng, proposes a novel methodology for intra-agency crime analysis based on modeling and implementation techniques from workflow management and information retrieval. A prototype system called "COPLINK Workflow" was implemented. In a user evaluation study involving 15 police detectives, they found the system useful for monitoring and collaboration purposes. The sixth paper, "Agents with Shared Mental Models for Enhancing Team Decision-Making" by Yen, Fan, Sun, Hanratty, and Dumer, presents a team-oriented agent architecture with an enhanced decision-making model. Through two sets of experiments in a simulated battlefield, they found the proposed decision-making approaches can be effective in improving team performance. The seventh paper, "Model Alignment of Anthrax Attack Simulations" by Chen, Carley, Fridsma, Kaminsky, and Yahja, describes their experience aligning two simulation models of disease progression attacks. They showed that the agent-based BioWar model can generate population level results that are close to the benchmark IPF epidemiological model. In addition, BioWar produces emergent properties that cannot be simulated in IPF. The eighth and last

paper, "Fighting Cybercrime: A Review and the Taiwan Experience" by Chung, Chen, Chang, and Chou, defines different types of cybercrime and reviews previous research and current status of fighting cybercrime in different countries that rely on legal, organizational, and technological approaches. The paper also presents an actual case study of cybercrime initiative at the Criminal Investigation Bureau of the National Police Administration in Taiwan.

5. Conclusion and future directions

The international and political landscape has been altered forever since the tragic events of September 11, 2001. Researchers have much to contribute to making the world a safer place. We believe national and homeland security research cannot take a short-term, reactive approach. It needs to be a long-term, concerted endeavor that involves committed researchers, practitioners, and policy makers. Researchers can contribute to the development and adaptation of counter-terrorism technologies. Similarly, we can help explore some of the critical privacy, confidentiality, and civil liberty issues of relevance to national security. We believe an open-minded and long-term approach to information exchange and understanding among the world's different cultures also could help identify the root causes of terrorism and contribute to making the world a more just and peaceful place.

References

- [1] H. Chen, R. Miranda, D. Zeng, T. Madhusudan, C. Demchak, J. Schroeder (Eds.), *Intelligence and Security Informatics, Proceedings of the First Symposium on Intelligence and Security Informatics, ISI 2003, Tucson, Arizona, June, Lecture Notes in Computer Science (LNCS 2665)*, Springer-Verlag, 2003.
- [2] H. Chen, Reagan Moore, D. Zeng, J.J. Leavitt (Eds.), *Intelligence and Security Informatics for National and Homeland Security, Proceedings of the Second Symposium on Intelligence and Security Informatics, ISI 2004, Tucson, Arizona, June, Lecture Notes in Computer Science (LNCS)*, Springer-Verlag, 2004.
- [3] National Research Council, *Making the Nation Safer: The Role of Science and Technology in Countering Terrorism*, Committee on Science and Technology for Countering Terrorism, The National Academies Press, Washington, DC, 2002.

- [4] Office of Homeland Security, The White House, "National Strategy for Homeland Security", 2002 (July). Office of Homeland Security. (2002). National Strategy for Homeland Security. Washington D.C.: Office of Homeland Security. Retrieved August 19, 2004, from the World Wide Web: http://www.whitehouse.gov/homeland/book/nat_strat_hls.pdf.

Hsinchun Chen
*Artificial Intelligence Lab. and Hoffman E-Commerce
Lab, Management Information Systems Department,
The University of Arizona, Tucson,
AZ 85721, United States*
E-mail address: hchen@eller.arizona.edu.