

Introduction to the Special Topic Issue: Intelligence and Security Informatics

Hsinchun Chen

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

Making the Nation Safer: The Role of Science and Technology in Countering Terrorism

The commitment of the scientific, engineering, and health communities to helping the United States and the world respond to security challenges became evident 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," (National Research Council, 2002, p. 1) explains the context of such a new 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.

A committee of 24 of the leading scientific, engineering, medical, and policy experts in the United States conducted the study described in the report. Eight panels were separately appointed and asked to provide input to the committee. The panels included: (a) biological sciences, (b) chemical issues, (c) nuclear and radiological issues, (d) information technology, (e) transportation, (f) energy facilities, cities, and fixed infrastructure, (g) behavioral, social, and institutional

issues, and (h) systems analysis and systems engineering. The focus of the committee's work was to make the nation safer from emerging terrorist threats that sought to inflict catastrophic damage on the nation's people, its infrastructure, or its economy. The committee considered nine areas, each of which is discussed in a separate chapter in the report: nuclear and radiological materials, human and agricultural health systems, toxic chemicals and explosive materials, information technology, energy systems, transportation systems, cities and fixed infrastructure, the response of people to terrorism, and complex and interdependent systems.

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 counterterrorism-related areas in IT: information and network security, the IT needs of emergency responders, and information fusion and management" (National Research Council, 2002, pp. 11–12). 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.

Cyberinfrastructure for Homeland Security: An NSF Workshop Report

After the release of the National Research Council report in 2002, many IT research communities have begun to contribute to the R&D in homeland security. The role that the emerging distributed cyberinfrastructure science might play

Accepted February 26, 2004

© 2004 Wiley Periodicals, Inc. • Published online 2 December 2004 in Wiley InterScience (www.interscience.wiley.com). DOI: 10.1002/asi.20116

in responding to unexpected events was explored in a workshop sponsored by the National Science Foundation (NSF). The University of California at San Diego hosted a group of 60 computer scientists, engineers, social scientists, and members of the emergency response communities on February 25–27, 2003 in La Jolla, CA to discuss the future applications of the cyberinfrastructure to homeland security and the most productive research and development environments in which to cultivate that potential. The workshop is an excellent example of how the IT research communities respond to the nation's (and the world's) need for security research.

Participants at the workshop viewed the cyberinfrastructure as a layer between fundamental technical components and emerging applications and a layer that empowers the federation of distributed resources (people, expertise, computational tools, data, information, and services). Four applications of the cyberinfrastructure that address critical homeland security needs were identified: (1) ubiquitous vision and sensing, (2) syndromic surveillance, (3) information integration, sharing, and visualization, (4) enabling the ecology of virtual organizations. Several recommendations were made in the workshop report, including those relevant to R&D in IT:

- NSF should encourage the development of fair use rules and their implementation in support of data sharing and data mining.
- NSF should promote research to advance our understanding of the couplings between the various distributed and decentralized sociotechnical systems that interact over the cyberinfrastructure.
- NSF should help develop community-based Living Labs to bridge the chasm between research and operations.
- NSF should support future research focused on uncovering the best practices of agencies concerned with national security.
- NSF should play a lead role in facilitating new partnerships among end users, technology providers, and basic science researchers as well as agencies concerned with national security to develop a consolidated scientific agenda and a coordinated program funding plan that can adequately serve the needs of the nation.

With the support of new federal programs, we have begun to see the emergence of excellent multidisciplinary, partnership-grounded research projects and joint academia–industry symposiums that bring together researchers, law enforcement and intelligence practitioners, and industry consultants and vendors.

Developing the Science of “Intelligence and Security Informatics” (ISI)

As one of the original founding mandates of the National Science Foundation in the United States, mid-to-long-term national security research in the areas of information technologies, organizational studies, and security-related public

policy is critically needed. Similar 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 science techniques need to be re-examined 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.

Long-term systematic technical, social, and policy research relating to intelligence and security informatics is critically needed, including but not limited to areas such as:

- Intelligence and security related content creation, management, and access
- Intelligence and security related information interoperability and sharing
- Intelligence and security related methodologies and best practices
- Policy and organizational studies in intelligence and security
- Intelligence and security related 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, event detection, and analysis

The first NSF/NIJ Symposium on Intelligence and Security Informatics (ISI 2003, <http://ecom.arizona.edu/ISI>) 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 in this kind of meeting.

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* (Chen et al., 2003). Many of the authors of the excellent research projects reported in the first ISI Symposium were solicited to contribute an expanded paper to this special issue.

With overwhelming interest and support from the community, the Second ISI Symposium was held in Tucson on June 10–11, 2004. 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.

In This Issue

This special issue consists of eight papers that report research in intelligence and security informatics. The first three are relevant to the social and policy aspects of intelligence and security informatics. “Technology, Security, and Individual Privacy: New Tools, New Threats, and New Public Perceptions,” by Strickland and Hunt, describes a project that surveyed a select group of citizens on the use of radio frequency identification (RFID) for business as well as homeland security purposes. The authors found a significant lack of understanding, and a significant level of distrust, even in the context of homeland security applications. There was a very significant consensus in favor of government regulation. The second paper, “User Acceptance of Intelligence and Security Informatics Technology: A Study of COPLINK,” by Hu, Lin, and Chen, presents a large-scale user study that empirically tested a factor model for examining law-enforcement officers’ technology acceptance. Based on an empirical examination targeting the COPLINK information sharing and analysis system and involving more than 280 police officers, this research found that efficiency gain and subjective norm appear to be significant determinants of perceived usefulness. In addition, perceived usefulness and perceived ease of use appear to be important determinants of an individual officer’s attitude toward COPLINK. A basic challenge for intelligence and security informatics is exploring the ways in which humans categorize or classify “sensitive” information. “Sensitive Information: A Review and Research Agenda,” by Thompson and Kaarst-Brown, reviews some of the dilemmas associated with classification of sensitive information, presents different classification approaches, and then identifies alternative propositions related to factors that influence judgment of degree of sensitivity.

The next five papers present technical, system, or quantitative research that addressed national security related issues. “A Semi-Supervised Active Learning Algorithm for Information Extraction From Textual Data,” by Wu and Pottenger, presents a semi-supervised active learning algorithm for pattern discovery in information extraction from textual data. The writers have successfully applied this learning technique to the extraction of textual features from police incident reports, university crime reports, and patents. The performance of their algorithm compares favorably with competitive extraction systems being tested in criminal justice information systems. “Automatic Crosslingual Thesaurus Generated From the Hong Kong SAR Police Department Web Corpus for Crime Analysis,” by Li and Yang, proposes a text-based approach to align English/Chinese Hong Kong Police press release documents from the Web. The research output consists of a thesaurus-like, semantic network knowledge base, which can aid in semantics-based crosslingual information management and retrieval. “Trust-Based Secure Information Sharing Between Federal Government Agencies,” by Liu and Chetal, proposes an interest-based trust model and an information sharing protocol, in which a family of information sharing policies is integrated, and information exchange and trust negotiation are interleaved. Implementation is compatible with the Federal Enterprise Architecture reference models. “Optimizing Anti-Terrorism Resource Allocation,” by Haynes, Kannampallil, Larson, and Garg, presents a three-part hybrid resource allocation model that uses multicriteria decision-making techniques to assess facility priorities, a utility function to calculate anti-terrorism project mitigation values, and optimization techniques to determine resource allocations across multiple, competing projects. The approach, model, and system have been evaluated using the cognitive walkthrough method with perspective system users in the field. The final paper, “Addressing the Homeland Security Problem: A Collaborative Decision-Making Framework,” by Raghu, Ramesh, and Whinston, presents a collaborative approach to providing cognitive support to decision makers by using a connectionist modeling approach. The connectionist modeling of decision scenarios offers several unique and significant advantages in developing systems to support collaborative discussions.

Conclusion and Future Directions

The international and political landscape has been altered forever after the tragic events of September 11, 2001. Researchers have much to contribute to making the world a safer place. We believe national 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 counterterrorism 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

- Chen, H., Miranda, R., Zeng, D., Madhusudan, T., Demchak, C., & Schroeder, J. (Eds.). (2003). *Intelligence and Security Informatics, Proceedings of the 1st NSF/NIJ Symposium on Intelligence and Security Informatics, Lecture Notes in Computer Science (LNCS 2665)*. Berlin/New York: Springer-Verlag.
- National Research Council. (2002). *Making the nation safer: The role of science and technology in countering terrorism, Committee on Science and Technology for Countering Terrorism*. Washington, DC: The National Academies Press.
- NSF Workshop Report. (2003). *Cyberinfrastructure research for homeland security*. San Diego, CA: University of California at San Diego.

About the Author

Dr. Hsinchun Chen is McClelland Professor of Management Information Systems at the University of Arizona and Andersen Consulting Professor of the Year (1999). He received a B.S. degree from the National Chiao-Tung University in Taiwan, an MBA degree from SUNY Buffalo, and a Ph.D. degree in Information Systems from New York University. He is the author of five books and more than 150 articles covering intelligence analysis, data/text/Web mining, digital library, knowledge management, medical informatics, and Web computing. He serves on the editorial board of *Journal of the American Society for Information Science and Technology*, *ACM Transactions on Information Systems*, and *Decision Support Systems*. Dr. Chen is a scientific counselor for the National Library of Medicine (NLM),

USA, and has served as an advisor for major National Science Foundation (NSF), Department of Justice (DOJ), NLM, and other international research programs in digital library, digital government, medical informatics, and intelligence analysis. He is the founding director of the UA Artificial Intelligence Lab and Hoffman E-Commerce Lab. The UA Artificial Intelligence Lab, which houses more than 40 researchers, has received more than \$15 million in research funding from NSF, NIH, NLM, DOJ, CIA, and other agencies over the past 10 years. The Hoffman E-Commerce Lab, which has been funded mostly by major IT industry partners, features state-of-the-art e-commerce hardware and software in a cutting-edge research and education environment. Dr. Chen has been a principal investigator (PI) of many major NSF Digital Library and Digital Government research programs. He is conference co-chair of ACM/IEEE Joint Conference on Digital Libraries (JCDL) 2004 and has served as the conference general chair or international program committee chair for the past six International Conferences of Asian Digital Libraries (ICADL), 1998–2003. Dr. Chen is also conference co-chair of the NSF/NIJ Symposium on Intelligence and Security Informatics (ISI) 2003 and 2004. His COPLINK system has been widely adopted in law enforcement (California, Arizona, Texas, Michigan, Massachusetts, Washington, etc.) and the intelligence community (CIA, NSA, and Department of Homeland Security) in the United States. COPLINK research has received several major law enforcement and government innovation awards and has been featured in various publications. Dr. Chen has also received numerous industry awards in knowledge management education and research including the AT&T Foundation Award, SAP Award, and the Andersen Consulting Professor of the Year Award.