By John Yen

EMERGING TECHNOLOGIES FOR HOMELAND SECURITY

ILLUSTRATION BY ROBERT NEUBECKER

The catastrophic events of September 11, 2001, dramatically demonstrated the reach and effects of terrorism and made protecting the security of citizens a top priority and a major challenge for many governments worldwide. The formation of the Department of Homeland Security is an exemplar response by the U.S. to such a challenge, drawing upon the intellectual and technological capabilities of scholars, scientists, and technologists. In this special section, we highlight some of the key emerging technologies related to several critical areas in the realm of homeland security.

As outlined in *The National Strategy for Homeland Security*,[1] the scope of U.S. homeland security is quite broad. Six of the mission areas considered critical include: intelligence and warning; border and transportation security; domestic counterterrorism; protecting critical infrastructures; defending against terrorism; and emergency preparedness and response. The first three areas focus on, among other things, preventing terrorist attacks against the U.S., the next two on reducing vulnerabilities within the U.S., and the last area on minimizing the damage and recovering from terrorist attacks that have occurred in the U.S. Information and communication technologies (ICTs) must play a pervasive, central role in overcoming the many inherent informational challenges embod-

[1] *National Strategy for Homeland Security*. U.S. Office of Homeland Security, July 2002; www.whitehouse.gov/homeland/book/.

ied within these six mission areas. Due to this wide scope, this special section seeks to provide a snapshot of some of the key emerging ICTs related to three of the mission areas (intelligence, protecting infrastructure, and emergency response). These three areas were selected because their informational challenges are not only critical but also highly interrelated.

The special section includes three articles on technologies to support intelligence and warning (including a summary by authors from the Defense Advanced Research Project Agency), two articles about protecting critical infrastructure, specifically cyber infrastructures (including an overview about technology and strategy for cyber security), and two articles regarding ICTs for enhancing emergency preparedness and response.

Intelligence and Warning

The article by Popp et al. surveys several DARPA-sponsored research thrusts for counterterrorism. These include: center-edge collaboration, analysis and decision support tools to support multi-agency information sharing and collaborative problem solving; ICTs involving transcription, machine translation, cross-language information detection and retrieval, and summarization, whose use will help to exploit the wealth of available foreign language speech and text; and pattern analysis tools intended to detect terrorist signatures from textual sources, representing and detecting patterns indicative of terrorist plots, and learning new terrorist patterns. The authors describe experiments conducted jointly by DARPA and several agencies within the U.S. intelligence and counterterrorism communities. The experiments, conducted by real intelligence analysts solving actual foreign intelligence problems using their own foreign intelligence data, indicated that analysts were far more productive using the IT tools provided by DARPA as opposed to using manually driven conventional means. Specifically, analysts spent much less time searching and preprocessing data (preparing data for analysis) and generating intelligence reports (summarizing analysis for decision makers) and much more time on doing the actual analysis (thinking about the problem).

Coffman, Greenblatt, and Marcus elaborate on one of the DARPA research thrusts for counter-terrorism: pattern analysis. More specifically, two graph-based techniques for detecting suspicious activities of terrorist groups are described: subgraph isomorphism algorithms (graph matching), and social network analysis (SNA). To better deal with the complex nature of terrorist activities, the authors enhanced traditional algorithms using these techniques to operate on graphs whose nodes and edges are labeled by attributes. Moreover, because intelligence data is often incomplete, ambiguous, and/or unreliable, these enhanced algorithms also consider inexact matches between the intelligence data and the pattern graphs. Based on the difference of social interactions between normal non-terrorist groups and those between terrorists, SNA metrics can be defined to characterize suspicious activities. Bayesian classifiers are then used to classify suspicious activity graphs and time-varying graphs.

Kogut et al. describe a research effort designed to support counterterrorism analysts using software agents that can dynamically anticipate their information needs. The approach is inspired by psychological studies suggesting effective human team behaviors are based on maintaining a shared mental model of the team. The authors use an agent architecture called CAST (Collaborative Agents Simulating Teamwork) to support a computational shared mental model about the structure and the process of the team, enabling software agents to dynamically anticipate information needs of analysts, and to assist them by finding and delivering information relevant to their needs.

Protecting Cyber Infrastructures

Both government agencies and global enterprises rely on a secure network infrastructure for sharing critical information and conducting business transactions; therefore protecting IT infrastructures from cyber attacks is critical. The article by Saydjari provides a general overview of the components of cyber defense, discussing a variety of challenges and issues ranging from strategies and technologies to performance assessment. One of the challenges discussed is the lack of an experimental infrastructure and rigorous scientific methodologies for developing and testing next-generation cyber security technology in support of deploying large-scale cyber security systems. The article by Bajcsy et al. describes a project with an extensive research agenda to address this very challenge. The goal of the project, which involves nine teams from academia and industry, is to create an experimental infrastructure network to support the development and demonstration of next-generation information security technologies for cyber defense.

Emergency Preparedness and Response

When a terrorist attack occurs, emergency response organizations and agencies at the federal, state, and local levels must quickly collaborate to assess the nature, severity, and effects of the attack, as well as to plan and coordinate their response actions. One of the two articles in this area focuses on wireless technology in support of first responders, while the other article describes the use of robotics technology for rescue operations. The article by Sawyer et al. describes a field study of police in Pennsylvania using mobile access technology to access an integrated justice information system. The goal of the study is to assess the potential impacts of 3G wireless networks on first responders. The authors' observations suggest that introducing wireless technology is unlikely to change existing organizational links within the legacy command, control, and communications infrastructure.

Murphy's article describes the use of robots after Sept. 11 in searching for victims and in assisting first responders in assessing the structural integrity of the World Trade Center foundation. The article discusses several research issues identified as a result of the experience: fundamentally, rescue robots must function within the physical constraints of complex environments and require special considerations for their mobility, sensing, and communication capabilities. Additionally, rescue robots must have good human-robot interaction to ultimately be accepted by the rescue workers.

Conclusion

It is fortunate the U.S. is able to utilize a wide range of technological bases to develop ICTs for homeland security purposes. This ability is tempered by the new problems and challenges raised by contemporary terrorist activities. In the articles that follow you will see both the tremendous science and the problems of operations that will bind the efforts to make the U.S. safer. Some of the challenges are due to the complex and secret nature of terrorist activities, while others are due to environmental constraints. The widely varying yet highly interrelated homeland security challenges discussed in this section are intended to help spur the global IT community in designing and developing novel and creative multidisciplinary solutions for such challenges. C

John Yen (jyen@ist.psu.edu) is a University Professor of Information Sciences and Technology and the professor in charge of the School of Information Sciences and Technology at Pennsylvania State University.

Communications of the ACM
~ 2004 Editorial Calendar ~

APRIL Etiquette for
Human-Computer Relations

MAY Transforming Financial
Services via ICT Architectures

JUNE Sensor Networks

JULY Medical Modeling

AUGUST Interactive Immersion in
3D Graphics

SEPTEMBER End-User Development

OCTOBER E-Voting

NOVEMBER Bioinformatics

DECEMBER Blogging and the
Ecology of the Internet