

Project Highlight: NSF Workshop on Cyberinfrastructure Research for Homeland Security

The role that the emerging distributed cyberinfrastructure science might play in responding to unexpected events was explored in a workshop sponsored by the National Science Foundation (NSF). The California Institute for Telecommunications and Information Technology (Cal-IT)² and the University of California San Diego, Jacobs School of Engineering hosted a group of about 60 computer scientists, engineers, social scientists, and members of the emergency response communities from February 25 to 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.

In plenary sessions, panel discussions, and breakout sessions for discussion by small working groups, participants explored the needs of the emergency response community and the potential contributions the cyberinfrastructure could make toward meeting those needs. Participants recognized that the impediments to implementation of cyberinfrastructure support of crisis management are not only technical, but also a matter of bringing together two communities that have different organizational cultures and different types of incentives for pursuing their work. To bridge this gap, participants proposed means by which the two communities could come together to develop effective, usable technologies that are likely to be adopted by the responder community.

Participants at the workshop viewed the cyberinfrastructure as a layer between fundamental components and applications; a layer that empowers the federation of distributed resources - such as people, expertise, computational tools and services, data, information sensors and actuators - to create virtual organizations or teams that reduce constraints of distance and time. Prodded by Dr. Peter Freeman's opening comments asking the workshop to "focus not on building the cyberinfrastructure, but on applying it," the participants discussed how the cyberinfrastructure might be used to support the unique needs of homeland security.

Four applications of the cyberinfrastructure that address needs that are critical to homeland security were identified. They were:

- Ubiquitous Vision and Sensing
- Syndromic Surveillance
- Information Integration, Sharing and Visualization
- Enabling the Ecology of Virtual Organizations

Seven recommendations were developed to help ensure that these potential applications of the cyberinfrastructure could become a reality. The first set of recommendations focus on five specific technical directions and approaches that were viewed as critical to the development of the cyberinfrastructure and its use in support of homeland security.

Recommendation 1 [Facilitate in-situ Cyberinfrastructure Research]: NSF should facilitate systematic, grid based, *in situ* research on cyberinfrastructure as an entity in itself. This research should emphasize experimental development of grid based, open systems and ensure the collection, archiving and sharing of data at various levels of abstractions ranging from packet flows to productivity enhancements.

Recommendation 2 [Promote Federation of Heterogeneous Networks]: NSF should promote experimental and theoretical research to support dynamic interoperability of highly diverse networks that federate, special and general purpose networks and help develop new societal scale services over this richly connected networking fabric.

Recommendation 3 [Develop Sensor Network Infrastructure]: NSF should support interdisciplinary research for the development of low cost, light weight, low power, rechargeable, remotely recalibratable, and mobile, field deployable sensor networks. Special emphasis should be placed on developing a modern sensor network software infrastructure that can be

incrementally upgraded and securely reprogrammed in complex and rapidly changing environments.

Recommendation 4 [Encourage Data Sharing, Mining and Analysis]: NSF should encourage the development of fair use rules and their implementation in support of data sharing and data mining. Experimental collaborative facilities to investigate data display and provide algorithmic and architectural support for Cyberforensics should be supported.

Recommendation 5: [Enhance understanding of Socio-Technical Systems]: NSF should promote research to advance our understanding of the couplings between the various distributed and decentralized socio-technical systems that interact over the cyberinfrastructure.

The next set of recommendations focused on specific approaches to bridging the chasm between the researcher community and the practitioners to ensure that innovations are responsive to the emergent needs.

Recommendation 6a: [Establish Living Labs] NSF should help develop community based Living Labs to bridge the chasm between research and operations. Social scientists should be strongly encouraged, if not required, to be a part of the teams that undertake research in homeland security.

Recommendation 6b: [Uncover Best Practices] NSF should support a study or fund research whose focus is to uncover best practices of agencies concerned with national security and disaster response to help identify what practices can be readily transitioned to state and local agencies and also identify the gaps that are unique to local and regional agencies

The final recommendation focused on mechanisms that might help with technology exchange and transfer across the various agencies and segments that share a common interest in homeland security.

Recommendation 7: [Facilitate New Partnerships] 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 and disaster response to develop a consolidated scientific agenda and a coordinated program funding plan that can adequately serve the emerging need.