Cyberinfrastructure Research for Homeland Security

-NSF Workshop Report

1 EXECUTIVE SUMMARY 1

2 INTRODUCTION 3

2.1 PURPOSE AND OBJECTIVES 3
2.2 ORGANIZATION OF THE WORKSHOP 4

3 FINDINGS 5

3.1 WHAT IS THE CYBERINFRASTRUCTURE? 5
3.2 WHAT UNIQUE HOMELAND SECURITY APPLICATIONS CAN BE ENABLED BY THE RIGHT CYBER INFRASTRUCTURE? 8
3.2.1 Ubiquitous Vision and Sensing 8
3.2.2 Syndromic Surveillance 8
3.2.3 Information Integration, Sharing and Visualization 9
3.2.4 Enabling the Ecology of Virtual Organizations 9
3.3 WHO ARE THE FIRST RESPONDERS AND CRISIS MANAGERS, AND WHAT TECHNOLOGY DO THEY NEED TO ENSURE THE MOST EFFECTIVE RESPONSE IN AN EMERGENCY? 11
3.3.1 First Responders 11
3.3.2 Crisis Managers 12

4 RECOMMENDATIONS 13

4.1 RESEARCH AND DEVELOPMENT 13
4.1.1 System Architecture Issues 13
4.1.2 Networks 15
4.1.3 Remote Sensors, Robotics, and PDAs 17
4.1.4 Data Sharing and Data Mining 19
4.2 BRIDGING THE CHASM BETWEEN RESEARCH AND OPERATION 21
4.2.1 Sociotechnical Systems 21
4.2.2 Living Laboratories 22
4.2.3 Community-Based "Testbeds" Built on Existing Technologies 22
4.2.4 Long-Term Commitment 22

5 POLICY ISSUES 23

6 MODALITY 24

7 REFERENCES 25

8 SUPPLEMENTARY MATERIAL 26

8.1 WORKSHOP ATTENDEES 26
8.2 WORKSHOP PROGRAM 26

Cyberinfrastructure Research for Homeland Security

-NSF Workshop Report

1 Executive Summary

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). Cal-$(IT)^2$ and the UCSD Jacobs School 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 contributions of technology 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 computer science research community 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.

At the workshop, participants defined 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 primary applications of the cyberinfrastructure were identified that address needs that are critical to homeland security. 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.

Recommendation 1: NSF should invest in systematic, grid based, *in situ* research on cyberinfrastructure as an entity in of 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: NSF should invest in experimental and theoretical research to support dynamic interoperability of highly diverse optical, copper and wireless networks segments, and to develop new societal services over this richly connected networking fabric. It is especially critical to systematically promote research to explore the connections, if any, between networking paradigms and the creation of social capital.

Recommendation 3: NSF should invest in interdisciplinary research to support the development of affordable light weight, low power, rechargeable, remotely recalibratable, and mobile field deployable sensors. 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. This infrastructure should also be able to support in-line analysis of video, audio and other sensor streams for rapid event detection and information retrieval and presentation.

Recommendation 4: NSF should invest in research to support 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: NSF should make long term investments in discovery-based Living Labs as well as community testbeds 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. NSF should also accelerate the development of crisis management and visualization centers for decision support and extend access to local agencies as part of the community outreach activities

Recommendation 6: NSF should partner with the appropriate agencies in supporting policy research to develop an understanding of what elements of cyberinfrastructure based systems developed for DoD applications can be readily transitioned into the civilian world and also uncover the unique gaps that remain to be filled. NSF should also play a lead role in facilitating a dialog among end users, technology providers and basic science researchers to identify the most important cyberinfrastructure needs of homeland security and help develop a scientific agenda that can adequately serve the societal need.

Recommendation 7: NSF should recognize that homeland security is not a linear extension of other ongoing scientific research activities. NSF should make a long term, persistent commitment to fund homeland security research.

2 Introduction

2.1 Purpose and Objectives

The National Science Foundation's program of distributed cyberinfrastructure is expected to accelerate to support large-scale scientific and engineering shared facilities for activities as diverse as astronomical observations and environmental monitoring. The National Science Foundation (NSF) plans to join the computer science community with scientific and engineering disciplines to build a high-performance, networked system of distributed computing, storage, visualization capabilities, and sensors on an unprecedented scale to create a new cyberinfrastructure with national, and ultimately global, presence. The purpose of this workshop was to explore the role of the distributed cyberinfrastructure in our response to unexpected events, both natural and of human origin.

It is easy to imagine scenarios in which unexpected occurrences trigger cascading events whose potential for death and damage can be mitigated if relevant information can be sensed and acted upon in a timely manner. Do the component technologies necessary to support this level of intervention exist today? What is missing? What cannot be done today by the crisis management or responder community that they believed could be enabled by the right cyberinfrastructure? These were some of the questions we set out to answer.

Imagine the following hypothetical scenario
The Chargers are playing the Cardinals at Qualcomm Stadium on a warm Santa Ana Sunday evening to a sell out crowd of 100,000, when the long dormant Rose Canyon fault fractures. The fans in the stadium feel a strong movement but there is no visible damage. Sensor arrays in the stadium have detected the seismic activity and camera feeds confirm that the structure is sound. But the crowd turns restless when the stadium lights flicker out. Unbeknownst to them, a dam on the San Diego River has breached and some of the 150 million gallons of stored water is forcing its way towards the stadium parking lot, built on the usually dry river bed. A reverse 911 system is triggered and prerecorded text and voice safety messages are fused in real time with information about the earthquake and the health of the stadium and delivered in a staggered manner to the fans' cell phones in the language of their choice, regardless of their cellular service provider. The quick delivery of relevant information and the ability to communicate averts a stampede. The fans are notified that they are safest where they are and are systematically polled to record their whereabouts, and prompted to leave messages and report unusual sights, sounds or smells. The community emergency system, which prioritizes text messages and reverse 911 polls to minimize system overload, has asserted its priority access rights and the preplanned federation of diverse telecommunication systems has taken place. The voice enabled exchanges that flow over this community system are rendered into text and recorded in a database that is rapidly building situational awareness for the entire southern California region.
Business rules and access mechanisms governing the use of this newly created dataset are already in place and the data set gets registered on the Cyberinfrastructure grid. A professor in Arizona, who develops specialized algorithms for anomaly detection, was watching the football game and logs on to the dataset. His algorithm filters out the many personal messages of reassurance being exchanged and uncovers that a number of callers, in the vicinity of the stadium, report that they smell gasoline. He feeds this alert back. It is widely known that 15 million gallons of gasoline are stored in tanks positioned three minutes upriver from the stadium. The specter of a flaming river of gasoline lapping at the stadium bleachers has long been a collective San Diego worry but cameras at the tank farm show that only one of the gasoline tanks has ruptured and GIS enriched computational models project that the combined flow of water and gasoline making its way to the stadium parking lot poses no threat to the fans. Live aerial snapshots from the blimp hovering overhead, is multicast to the fans' cell phones to provide visible evidence that there is no threat to the fans.

2.2 Organization of the Workshop

To generate adequate discussion, the workshop organizers sought the ideas and opinions of experts from computer science, engineering, and social and behavioral sciences along with those in crisis management and homeland security. This included researchers who create, develop and deploy new systems as well as practitioners who use the technologies. Industry, universities and the local, state, regional and national agencies were well represented. Our goal was to engage this important community early in the deliberations so that their distinct needs could be incorporated into the architecture of the distributed cyberinfrastructure. The workshop organizers, in consultation with representatives from NSF, invited about 60 participants [1] with expertise in the following fields:

- Crisis management on local, state, and national levels
- Design and deployment of arrays and networks of sensors
- Network design and architecture
- Grid computing
- Establishment and management of large, distributed data sources
- Data mining
- Systems analysis
- Models for collaboration among scientists and engineers, and between technology researchers and end users (practitioners)
- Information security
- Ethical use of information
- Management of technological enterprises
- Advancement of national information infrastructure, such as the Internet.
- Management of government science and technology initiatives
- National and international science and technology policy

The workshop, hosted by Cal-(IT)[2] and the UCSD Jacobs School, convened in La Jolla, California on the evening of 25 February 2003 and adjourned mid-day on 27 February 2003. Plenary sessions and panel discussions were held on a series of topics. The plenary speakers included Larry Smarr, Joel Birnbaum, Peter Freeman, Priscilla Nelson, and Frieder Seible. Five panel sessions were organized on Mobile and Ad-hoc Infrastructure, Fixed Infrastructure, Security, Data/Grid and Collaboration and Decision Support. Breakout working groups, which reported back to the group as a whole at the end of the workshop, were organized around the same thematic lines. A wrap-up panel provided summary comments on the working group reports and on the workshop as a whole.[2]

The workshop findings are presented in section three followed by the recommendations in section four.

[1] Organizers and participants in the workshop are listed in Appendix A.
[2] The agenda for the workshop is provided in Appendix B.

3 Findings

3.1 What is the cyberinfrastructure?

Two recent studies provide some answers to the question "What is the cyberinfrastructure?" President Bush's "National Strategy to Secure Cyberspace" released about two weeks before the workshop, notes that:

> For the United States, the information technology revolution quietly changed the way business and government operate. Without a great deal of thought about security, the Nation shifted the control of essential processes in manufacturing, utilities, banking, and communications to networked computers. As a result, the cost of doing business dropped and productivity skyrocketed. The trend toward greater use of networked systems continues.
>
> By 2003, our economy and national security became fully dependent upon information technology and the information infrastructure. A network of networks directly supports the operation of all sectors of our economy—energy (electric power, oil and gas), transportation (rail, air, merchant marine), finance and banking, information and telecommunications, public health, emergency services, water, chemical, defense industrial base, food, agriculture, and postal and shipping. The reach of these computer networks exceeds the bounds of cyberspace. They also control physical objects such as electrical transformers, trains, pipeline pumps, chemical vats, and radars.

- CI is a layer between fundamental components and applications. It empowers the federation of distributed resources (people, expertise, computational tools and services, data, information sensors, actuators) to create virtual organizations or teams (grid communities, collaboratories) that reduce constraints of distance and time. (Distance= geo, organ., disciplinary…). CI is a means to an end…
- CI involves finding and supporting commonality of use, encapsulating best practice, interoperability, making it easier, more cost-effective for a wide range of applications with specific requirements, participants, etc.
- Overall theme: the need for *integration*, across technologies and across organizations
- The issues are not all technical; *people* and organizational dynamics count
- *Ease of use* and accessibility are critical; great technology, if not used, is not great
- *Robustness* is critical; the mobile cyberinfrastructure is only effective if it actually works during a crisis
- *....A new area: we shouldn't propose short-term fixes to the infrastructure for first responders, but scope out long-term grand-challenge problems*
- *....Not a 3-5 year solution, despite the premise!*

Our Nation's critical infrastructures are composed of public and private institutions in the sectors of agriculture, food, water, public health, emergency services, government, defense industrial base, information and telecommunications, energy, transportation, banking and finance, chemicals and hazardous materials, and postal and shipping.

> Cyberspace is their nervous system—the control system of our country. Cyberspace is composed of hundreds of thousands of interconnected computers, servers, routers, switches, and fiber optic cables that allow our critical infrastructures to work. Thus, the healthy functioning of cyberspace is essential to our economy and our national security.

The NSF Blue Ribbon Advisory Panel on Cyberinfrastructure concluded a few months ago that

> "a new age has dawned in scientific and engineering research, pushed by continuing progress in computing, information, and communication technology, and pulled by the expanding complexity, scope, and scale of today's challenges. The capacity of this technology has crossed thresholds that now make possible a comprehensive "cyberinfrastructure" on which to build new types of scientific and engineering knowledge environments and organizations and to pursue research in new ways and with increased efficacy."

At the workshop, participants defined 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. Distance in this context could be measured geographically, organizationally, or in a disciplinary sense. Cyberinfrastructure was seen as a means to an end and involved finding and supporting commonality of use, encapsulating best practice, enabling interoperability, making it easier, more cost-effective for a wide range of applications with specific requirements and participants.

It appears that the emergence of cyberinfrastructure predates efforts to define it. We continue to struggle to find words to describe and circumscribe this phenomenon probably because it was not engineered to predefined specifications. Instead the cyberinfrastructure evolved in an organic manner. The scale, scope and nature of this phenomenon likely surprises even those that worked closely on creating pieces of it. A somewhat pointed example of the evolutionary nature of the cyberinfrastructure pertains to its definition. As of this date, neither the Oxford English Dictionary nor the Webster's Dictionary has an entry for "cyberinfrastructure," but the cyberinfrastructure is now capable of defining itself! Googlism.com, which reveals "what Google.com thinks of you, your friends or anything," catalogs the following googlisms for cyberinfrastructure. These definitions suggest that Google may be classifying people who influence the cyberinfrastructure as part of the cyberinfrastructure!

In any event, because of its organic nature, the future evolution of the cyberinfrastructure can be significantly influenced by the manner in which it is used and the support that is provided for particular enhancements. Against this implicit backdrop and 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 cyberinfrastructure might be used to support the needs of homeland security.

"What is Cyberinfrastructure?"
–excerpted from Googlisms.com.

- cyberinfrastructure is the elimination of arbitrary limits on the scope and scale of research activity
- cyberinfrastructure is the linkage of computational and data resources with sensors and instruments
- cyberinfrastructure is a way to share data and tools in real time
- cyberinfrastructure is a network of knowledge
- cyberinfrastructure is revolutionizing earthquake engineering

- cyberinfrastructure is planning to recommend a substantial federal initiative in this area
- cyberinfrastructure is recommending major increases in the support for cyberinfrastructure

- cyberinfrastructure is now available

3.2 What unique homeland security applications can be enabled by the right Cyber Infrastructure?

Four key applications emerged from the discussions. These applications are at the intersection of the capabilities attainable within the cyberinfrastructure framework that also address needs critical to first responders.

3.2.1 Ubiquitous Vision and Sensing

Vision, and more generally sensing, is a natural way of building situational awareness. In the past, communities used human observers, animal sentinels and other improvised devices to guard themselves from threats. Today, technology can help serve the same basic societal need in a more comprehensive and cost effective manner. Currently there are numerous camera networks and other mission specific sensor deployments in the field. They tend to be costly and limited in their capabilities and are largely not digitally networked. Consequently, much of the data gathered by these sensors is never analyzed and very little of it is used to build and develop long-term awareness of our physical spaces. There is also much useful information that can be created by fusing multi-sensorial data from multiple audio, video, and other sensors with archived information such as aerial images. In this context, it will be critical to systematically translate, transcribe and alter the representation of the data in real time and also incrementally update these datasets in real time as a crisis unfolds. Our ability to gather data for situational awareness is likely to be dramatically enhanced through the use of robots that are digitally tethered to the cyberinfrastructure. By serving as mobile extensions of the cyberinfrastructure, robots are likely to significantly alter the acquisition and delivery of information and also start to serve as versatile actuators. Recognizing that persistent networking, data archiving, processing and analysis are essential attributes of the cyberinfrastructure, we conclude that ubiquitous sensing and vision could represent a new large scale application of the cyberinfrastructure in support of homeland security.

3.2.2 Syndromic Surveillance

Today, over 90% of the nation's medical records are maintained on paper. This results in numerous medical errors and inconsistent quality of care. Current practice also relies on trained human observers to pick out suspicious patterns of activity. The islands of medical information that do exist today are beset by the usual problems of one-of-a-kind systems. There is a dire need for a comprehensive knowledge-based network of distributed interoperable systems that can provide information for sound decisions about health when and where needed. If fully implemented, such a system may rectify many of the errors[3] endemic to paper based approaches. It may also help detect the effects of a bioterrorism attack or a naturally occurring epidemic very early, by noting a pattern of only a few anomalous cases that cluster within a short time frame or geographic area (National Committee on Vital and Health Statistics, 2000). Such capability will save lives, and by heading off a larger catastrophe, conserve resources devoted to emergency response.

[3] The Institute of Medicine estimates that 44,000 to 88,000 preventable deaths occur every year due to poor medical records and the cost of medication errors is estimated to be in excess of $76 billion/year.

With some additional enhancements, the cyberinfrastructure is well poised to support such a National Health Information Infrastructure. The cyberinfrastructure provides many examples of large scale data organization, storage, retrieval and data mining. The distributed systems that underpin the cyberinfrastructure can be suitably scaled to support health care applications, but close attention will have to be devoted to ensure patient privacy and help build public confidence in the system.

3.2.3 Information Integration, Sharing and Visualization

Situational awareness information is already being gathered by a diverse collection of entities. Some organizations gather information over a long period of time and maintain datasets of extraordinary quality, resolution and reliability. Yet, in spite of the rapid advances in networking and telecommunications, current policy, processes and systems do not allow communities that share a common purpose or mission, such as crisis response or rescue, to share and access data in a systematic manner. Hurdles to overcome in this regard range from organizationally induced policy barriers to lack of interoperability in the technical systems used for sensing, processing, archiving, networking and display of data. While technology can sometimes force policy changes through disruptive influences, it can also serve the needs of well articulated, policy driven initiatives. Success in overcoming these hurdles will further elevate our capabilities in gathering, archiving and using data.

A number of emerging developments point to the potential role of the cyberinfrastructure in this regard. Data networks, such as the Internet, were initially an overlay over the preexisting circuit switched world of telecommunications. During the last decade, as the cyberinfrastructure took root, large segments of the telecommunication systems have morphed into a network whose core is IP based. Systems that are now supported over core IP networks include centrally managed cellular, land line and satellite based networks as well as more amorphous, but pervasive, wireless systems based on the unlicensed band. A handful of new initiatives are underway that field an IP resident unified infrastructure for accounting, authorization and authentication for multiple commercially competing air interface alternatives. This implies that diverse telecommunication systems can now be easily bridged over the cyberinfrastructure. In the world of software systems, XML has taken root as a common language for data representation and UML as a language for specifying systems. The cyberinfrastructure stands poised now to support the rapid recomposition of entire systems including the datasets they rely on, and to deliver it over the transport network of the responder's choice. In order for data and information so delivered to be effective in decision support, it is necessary to visualize that information. Current approaches to visualization don't provide the tools and facilities to allow users from multiple sectors to collaboratively assess, plan and execute their missions. There is a need to enhance the cyberinfrastructure with first responders' decision support tools that allow visualization of situational awareness data in a manner that adapts itself to the end viewer's needs. Real-time analysis tools are also needed to facilitate collaboration across multiple sectors using different kinds of appliances.

3.2.4 Enabling the Ecology of Virtual Organizations

The last of the four applications is different from the first three. Here the emphasis is on evolving the cyberinfrastructure in a manner that allows for recurring large scale drills that bring together

collaborators from multiple sectors to confront a simulated threat. There is a history of conducting disaster preparedness drills in a real world setting with actors playing the roles of victims. It is important to recognize that many of the elements of control and the basis of decision making will increasingly reside on the cyberinfrastructure. Rather than viewing the cyberinfrastructure as providing data to drive an external drill, the suggestion here is to host the drill within the cyberinfrastructure. Hence, there is a need to build in mechanisms to virtually cordon off a "segment" of the actual cyberinfrastructure to conduct these cyberdrills. An added value that would accrue from such exercises is the training of the community of users and the creation of a new ecology of virtual organizations. This community would generate feedback that would help develop new practices and uncover unmet needs.

Against this backdrop it is worth exploring the nature and role of the first responders and crisis managers.

How to enable the ecology of virtual organization for HLS using Cyber Infrastructure?

- Must be done in real time
- Must be dynamic
- Must use imperfect knowledge; uncertainty
- Must include multi-disciplinary groups

Identification

- Lead generation
- Spider analysis (decision analysis)
- Natural language/video/graphical searches
- User profiling
- Text mining
- Automated probes
- Cataloging; validation
- Sensors

Recruit/Negotiate

- Authentication
- Encryption
- Interoperability
- Compensation/incentives
- Indemnification
- Fair issues
- Accountability
- Authorization (limited scope)
- Culture change

Implementation

- Interoperability
- Communication, databases, semantics
- Decision support system
- Transparency
- Usability (interfaces)
- Rich media (audio/video)
- End-to-end performance
- Reliability
- Cost
- Search fidelity
- Sensor

Authorities

- Existing C & C Plans
- Adapt existing plans
- Create Plans in real-time
- Resource ID & Tracking
- Decision Support System

3.3 Who are the First Responders and Crisis Managers, and what technology do they need to ensure the most effective response in an emergency?

3.3.1 First Responders

The initial response to any threat usually comes from ordinary citizens. Something explodes or catches fire, a gas wafts through a subway station and riders begin to collapse, a highway bridge or a building falls, and whoever happens to be on the scene responds. These initial responders can be any member of the public; they are likely to be untrained in emergency response, and they may not be literate in any language. In most instances, the initial responder would simply call 911. If, however, the initial responders are themselves trapped in a collapsed building or in a subway tunnel between stations, for instance, other means of communicating the nature of the emergency would be useful. For example, geolocatable devices that could be used for two-way communication could be placed in public areas in which they are likely to be needed, such as subway trains and public buildings.

The term first responder usually refers to individuals with specific training in emergency response such as firefighters, emergency medical technicians (EMTs), paramedics, and police officers. The educational background and training required to be firefighter, EMT, or police officer is specific to their mission and short term, as little as one month for EMTs and as little as 6 months (in the academy) for police officers. All responders at the scene are likely to be under stress and possibly endangered themselves. Therefore, the developers of new technology need to provide the information first responders need to make immediate decisions in the simplest usable format since excess information or information that is difficult to process or understand will hinder the response.

The conditions under which emergency responders operate pose additional challenges to the design of technology they will use. For example, equipment designed for use by firefighters should be waterproof. It should also be safe to operate in an explosive atmosphere, around a natural gas leak for example. A recent report (FEMA, 2003) estimates that nationally, firefighters have enough two-way radios to equip fewer than half the firefighters on any given shift and that very few of those are waterproof or safe to operate in an explosive atmosphere. In order for new technology to widely be used, it will also have to be more affordable than the best available technology is currently. Even in the wake of the terrorist attacks of September 11, 2001, funding for the nation's firefighters and police has not expanded to the point were they can all afford the best currently available technology. Additional money for this venture will be a matter of national will and political action. However, those designing the next generation of technology could help the cause by making low cost a design goal.

The experience of the men and women who currently serve as first responders is a valuable resource to those who are designing new technologies for their use. Including first responders from the initial stages of design to the deployment of new technology is critical to developing the best possible technology and to assuring that that technology will be adopted and used.

3.3.2 Crisis Managers

The third tier in the response to unexpected events is formed by crisis managers. Their missions extend beyond the immediate response to events; instead they are responsible for managing a cycle of responsibilities that includes preparation for emergencies, detection of adverse events, emergency response, recovery, and mitigation or prevention. Cyberinfrastructure research and development could contribute to advancement in each of these phases of crisis management.

Because crisis management often crosses from local to regional, state, federal, and even international levels, coordination of information is essential. During the response phase of a crisis, managers at all levels need to coordinate information from disparate sources to both assess the situation and decide how to allocate finite resources.

Events that require such a coordinated response tend to incur widespread disruption, of the power grid, for example. In addition, the cyberinfrastructure itself may be damaged. Cables carrying internet and telephone transmissions may be cut; wireless network transmission towers may be toppled. These effects are often compounded as individuals in and outside of the affected areas flood existing communications channels in order to gain information or to communicate with each other. Therefore, the information systems on which crisis managers rely must be particularly robust and based on redundant systems so that if one component fails, another may take its place.

Decisions in an emergency must often be made quickly and need to be based on accurate, current information. Cyberinfrastructure for decision support requires the ability to provide constant, accurate updates. Real-time streaming video and audio transmitted by responders or remote sensors onsite would partly serve this need. In addition, crisis managers may need access to information that is normally proprietary, such as building plans, or that is normally the domain of another government agency. In order for that information to be rapidly available, policies and procedures for sharing the information must be in place prior to the emergency.

Finally, in the context of human factors research in the use of technology for decision-making in an emergency, some information can be gained by studying how crisis managers used technology during an actual emergency, after the event (cf. Huyck and Adams, 2002).

4 Recommendations

4.1 Research and Development

4.1.1 System Architecture Issues

Cyberinfrastructure systems have gradually evolved over the last three decades. Although they are now beginning to be seen as an integral system, they were largely created as a loose federation of specialized systems for computing, storage and visualization. These systems gradually became enmeshed with each other and with specially commissioned digital libraries and other distributed repositories of data. This then led to the birth of advanced search tools for the dynamic cataloging of the ever growing corpus of data. Many societal systems, such as banking, power, education, transportation and law enforcement are now reforming themselves over the cyberinfrastructure. Yet, even as our dependence on cyberinfrastructure grows daily our understanding of cyberinfrastructure as an entity remains very limited and grossly inadequate, especially in the context of homeland security.

System Architecture Issues

- From Component to systems research
  - systems research needs major boost in funding
  - ITRs are move in this direction
  - Need for continued innovation in high end components, not just use of commodity pieces
- Study Cyberinfrastructure Systems as an object of interest
  - How they scale and fail
  - You can't protect your infrastructure if you don't know what it is
  - Public archives of data on CI
- Build Grid Systems for
  - Many people with short time horizons
  - Few people with large data sets
- Systems that are open, open, open

- What is the capacity of the current cyberinfrastructure?
- What regulatory mechanisms govern its growth?
- What metrics might predict its health?

Cyberinfrastructure systems pose a particular challenge in that its evolution occurs under the influence of an uncontrollable and sometimes unobservable set of temporal forces. Just as with seismic studies and evolutionary biology, a good deal of the cyberinfrastructure research will have to be conducted *in situ*. To make this possible, we believe that it is critical to instrument the cyberinfrastructure extensively so that one can measure the "state" of the cyberinfrastructure at numerous levels of abstraction from packet flows to productivity and trust enhancements. We must also continue experimentation with new services, architectures, protocols and technologies while acknowledging that these experiments will yield the most insight when they are done *in situ* on the Grid. Such experiments are likely to be difficult to design and expensive to execute and so the national interest would be best served if these systems are ***open***.

Crisis management is a particularly demanding application of the cyberinfrastructure. During disasters parts of the cyberinfrastructure itself may be damaged, and the rest of the infrastructure

on which the cyberinfrastructure depends, most notably the electrical grid, may also fail. Systems used for crisis management should have failsafe modes of operation and research is needed to identify the critical features required for such emergency management and find ways to provide that during an emergency.

At present, we don't have a very good understanding of how the Internet behaves under crisis conditions (CSTB, 2002b), in part because data are not collected neither during normal operation nor during system-taxing events. Furthermore, data tends to be discarded quickly, within a few months. Study of how the cyberinfrastructure functions as a system will require broader and deeper data collection that emphasizes continuity, consistency, and archiving of results. This work will need to find and maintain a delicate balance among disclosure, privacy, and security.

Means to study the Internet:

1. Map the topology of routers using snapshots, history and archives.
2. Extend the topological maps to Internet hosts, network access points (NAPs), firewalls, and links.
3. Annotate maps to understand vulnerabilities
4. Map software such as ports, services, and middleware.
5. Census the domain names and IP addresses in use
6. Characterize the traffic over the Internet.

Recommendation 1: NSF should invest in systematic, grid based, *in situ* research on CI 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.

4.1.2 Networks

In recent years, as data centric services have became more dominant, wireless, wireline, cellular and decentralized networks have melded together in an ad-hoc manner to sustain the demand for information exchange ranging in scale from short bursts of SMS to collaborative visualization of large scale data sets. Familiar design requirements such as scalability, self configuration, and robustness have to be reengineered over a vastly more diverse network that incorporates ultra-high-rate optical core networks that interconnect frequency agile, interference prone, software defined, wireless access networks with dense sensor array deployments.

Networking Issues

- Robust Redundant Networks
  - Key Is That They Always Work
  - System Approach Integrating Wireless, Optical, Copper Networks
  - Systems Approach To Network Vulnerabilities
- New Technology Coming in Optical and Wireless Networks
  - Work on Interoperability of Existing Networks
  - Needs For PVNs
  - Advanced Concepts May be Useful For Large Data Sets
- Systems For Communication To Public Needed
- Focus on robustness / scalability of wireless communications: redundancy, anti-jamming capabilities, self-configuration / self-healing infrastructures
- Networks that are scalable and reconfigurable
- Systems that do not depend on existing infrastructure … but may use it.
- Use alternate protocols? Frequencies?
- Needs during crisis may require different features than standard protocols.

The rich interconnectivity between these networks and the built in self healing mechanisms can create large unexpected surges in traffic especially after an unexpected event when large parts of the infrastructure may have been destroyed or when denial of service attacks are deliberately launched. How do we architect networks to ensure readiness and interoperability despite large scale, possibly coordinated attacks? Conversely are there cost effective network architectures that can transform themselves dynamically (by selecting alternative forms of information representation or using alternative protocols over an altered topology) to cope with prevailing conditions in a secure manner? Early signs of abnormal activities are likely to be observed over the new cyberinfrastructure. It is therefore critical to develop advanced societal scale group communication systems that generalize the notion of the emergency broadcast system.

With the growing maturity and pervasiveness of information networks, NSF should take a more active position in funding research that examines the interrelationship between social networking and information networks. Of special note is the concept of Social Capital that has regained prominence after Robert Putnam published his book, “Bowling Alone” [2000, Simon and Schuster] Putnam’s work provides a rare opportunity for researchers, who are immersed in perfecting the finer technical details of a network, to pause and take note of the societal impact of their work. Putnam opines that:

> *Whereas physical capital refers to physical objects and human capital refers to the properties of individuals, social capital refers to connections among individuals – social*

> *networks and the norms of reciprocity and trustworthiness that arise from them. In that sense social capital is closely related to what some have called "civic virtue." The difference is that "social capital" calls attention to the fact that civic virtue is most powerful when embedded in a sense network of reciprocal social relations.* ***A society of many virtuous but isolated individuals is not necessarily rich in social capital****.*

So one might assume that information networks automatically generate social capital by networking individuals and communities. Yet there is evidence that Internet based connections might be displacing community based connections and thereby destroying the community's social capital. If the Cyber Infrastructure is to help bring well knit communities of first responders together, we must make certain that technology innovations that help cope with rare events do not disrupt the civic virtues that help handle the everyday problems.

Recommendation 2a: NSF should invest in experimental and theoretical research to support dynamic interoperability of highly diverse networks that federate, special and general purpose networks composed of optical, copper and wireless segments and to develop new societal services over this richly connected networking fabric.
Recommendation 2b: NSF should systematically promote research to explore the connections, if any, between networking paradigms and the creation of social capital.

4.1.3 Remote Sensors, Robotics, and PDAs

Developing mobile and ad hoc elements of the distributed cyberinfrastructure offers particular promise for responding to unexpected events. Currently we rely largely on human responders using two-way radios. The development of a distributed, ad-hoc, rapidly deployable and re-configurable cyberinfrastructure will enable access to locations too dangerous for or inaccessible to humans. Remote sensors will provide previously unavailable views within disaster sites providing a more complete view of the scene and enabling a more effective response. These remote sensors will need to be networked to provide flexible tools for monitoring ongoing events.

Remote Sensors, Robotics, and PDAs

- Creating A Densely Instrumented World
  - Temporally And Spatially Dense Sensornets In Complex Obstructed Environments
  - Local On-board And Collaborative Processing
  - In-line Analysis Of Data Streams, Alerts And Decision Support
  - Rapid Deployment Of Ad Hoc Infrastructure
- Large Arrays Of Intelligent Video Streams
  - Realtime Remote Inspections W/ Streaming Video/Audio
- Robotic Components
  - Dropping New Sensors In Inaccessible Places
  - Data Mules
  - Delivering Energy To Remote Sites
- PDAs For Initial Damage Estimates
- Smart Tags With Microphones And Sensors

- Develop adaptive signal processing, data filtering and analysis in the network to manage information overflow

- Need for new kinds of actuators/sensors/robotic nodes (biological, chemical, explosive, wind data, etc.)
- More usable video surveillance, intrusion detection, automated monitoring

A wide variety of new sensors could be useful for crisis management. They include biological sensors, to detect harmful microorganisms, humans trapped within debris, or blood oxygenation levels through fingertip monitors; chemical sensors to detect harmful agents, intentionally or accidentally released, or explosive materials; monitoring sensors to record local air flow or temperature; and radiation sensors. Many of these are currently available, but deployment of large numbers of sensors to create temporally and spatially dense networks of unmanned sensors will require improvements in cost and durability.

The most robust and flexible sensor networks will need to rely on mobile nodes for deployment into dangerous and inaccessible areas. These robots would function as self-positioning sensors that deliver the sensing capability to needed locations. They could also find pathways through debris fields, deliver power to remote sensors, or retrieve data. The robots used for emergency response will need to be particularly robust, able to withstand harsh physical conditions in which power may not be readily available. They will need to be able to position themselves optimally with respect to other sensors and to the environment, to both sense and maintain communication in rough terrain. The development of these sensors will require

interdisciplinary teams from chemistry, biology, materials science, engineering and computer science to work together to create low cost, light weight, low power, remotely recalibratable, rechargeable, mobile, field deployable sensors.

While the role and value of individual sensors is reasonably well understood, the capabilities of ***networks*** of sensors fail to match the sophistication of networks of computers. Techniques need to be developed to transform sensor networks from today's single mission, stand alone, stove pipe system to a more modern infrastructure that can be incrementally upgraded and securely reprogrammed in complex and rapidly changing environments.

The drive to lower the cost, weight and power consumption of the next generation of field deployable sensor networks will require much closer exploration of the design tradeoffs including the aggressive use of local and collaborative computation and communication to support in-line analysis of data streams.

Recommendation 3: NSF should invest in interdisciplinary research to support the development of low cost, light weight, low power, rechargeable, remotely recalibratable, and mobile, field deployable sensors. 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. This infrastructure should also be able to support in-line analysis of video, audio and other sensor streams for rapid event detection and information retrieval and presentation.

4.1.4 Data Sharing and Data Mining

There are two aspects of data sharing that require special attention. Data sets often reside in silos that are isolated from each other due to jurisdictional boundaries or representational incompatibilities. Most of these problems are not technical.

The most important change required to overcome these barriers is to build trust between organizations. This will require the establishment of rules for the fair use of data, compensation for data provided, indemnification of data providers, and assurance that the act of sharing data will not result in its corruption.

Given the nature of the threat to homeland security, regional, cross-institutional data sharing is necessary.
Policies and procedures for sharing information must be established prior to an emergency. Access to sensitive databases could be on a contingency basis, with authorization granted, or not, depending on context.

Data Sharing and Data Mining

- Grid Federation Of Diverse Data Resources
  - Data To Information To Intelligence
  - GIS→Imagery
- Sharing Data Across Institutional Stovepipes
  - Regional Data Sharing Is Necessary Given Nature Of Threat
  - Primarily Institutional Problems—not Technology
  - Building Trust Relations Between Data Silos Is Most Important
  - Fair Use Of Data Rules
- Networked Decision Support Centers
  - Response Management Display Systems
  - Usability Of Data Visualization
  - Decision Support Software Systems
- Fusion and decision support
  - Cope with faulty information
  - Need to push updates to past decisions
  - Must be intuitive and high-level.
  - Include cognitive support.
- Usable with minimal training
  - Multilingual, possibly icon-based
  - Many adults are not literate in any language
  - Better support for real-time information sharing, integration and collaboration, across platforms
- Dynamic policies based on need and strong authentication
- Need fast, emergency access to disparate, proprietary databases
- Need to limit outside access (press, other units, government)
- Needs to cover intergovernmental use, Including international (e.g., Seattle/Vancouver)
- Cyberforensic support.
- Strong audit
  - For abuse response
  - For tracking decisions
- Security And Privacy
  - Local First Responders May Not Need Encryption
  - Automated Network Security Assessment Tools
  - Security Is Relevant To A Context and
  - Emergent Behavior Is Important Between Systems

As sensor arrays become ubiquitous and information systems proliferate, they will make available vast amounts of data. The extraction of intelligence from this corpus of data and presenting it in a useful format to decision makers is quite a challenge. Research activities that are needed in this context include the use of probabilistic concepts to iteratively extract useful information and intelligence from unreliable data.

Intuitive decision support systems that require little or no training to use will be invaluable to decision makers operating under conditions of elevated stress as well as when groups drawn from multiple agencies collaborate. The use of multilingual, possibly icon based presentation formats will be critical to the effective use of this system. Data in an emergency can grow old quickly. Design of decision-support systems will require means to push updates, to make users aware of when they need to re-evaluate the situation and system. Research in this regard will benefit from the fielding of multi-sector collaboration centers where advanced concepts can be prototyped and user feedback carefully gathered.

Security and privacy concerns are likely to vary dramatically during a crisis. Research is needed to develop mechanisms that can flexibly provision varying levels of security and privacy along with provably enforceable safeguards that will inspire confidence in the people whose lives are likely to be affected by these policies. Cyberforensic support must be designed into the cyberinfrastructure infrastructure for abuse response and tracking the factors that led to specific decisions.

Recommendation 4: NSF should invest in research to support the development of: fair use rules and their implementation in support of data sharing, algorithms for data mining, experimental collaborative facilities to investigate data display and provide algorithmic and architectural support for Cyberforensics.

4.2 Bridging the Chasm between Research and Operation

As with other large scale socio-scientific systems, such as universal immunization, new scientific capabilities take a while to diffuse into and become an integral part of the social fabric. Throughout the workshop, participants repeatedly noted a large cultural gap between the research community and the operational community. Each group uses specific vocabulary and language to describe their work which is not shared by or familiar to the other. The nature of their missions is different as well. The research community is often seeking ideal solutions to intellectually interesting problems, whereas the operational community seeks adequate solutions to immediate and pressing practical problems. The two can come together, but doing so will require mutual accommodation and learning.

Bridging the Chasm between Research and Operation

- Community Testbeds Built On Existing Technologies
  - Create Local Teams Of Technologists And Community
  - Incentive Grants To Groups Of Organizations That Build Trial Demonstration Programs In Key Metropolitan Regions At High Risk
- Living Laboratory Characteristics
  - Need Real Experimental Systems With Evaluation By End Users
  - Rapid Prototyping Cycles With Users Involved In Each Iteration
  - Can Monitor Large Engineered Physical Systems Or Environment
- Socio-technical Systems And Professionals
  - Interdependent System of Social Scientists Working With Technologists
  - Rapid Creation Of Virtual Organizations Devoted To Crisis Management
- Need to "train as you use"
- Whole system training, simulation and testing
  - Include red-team testing.
- Testing should build public trust prior to use
  - Accelerate the development of new hands-free capabilities for first responders
  - Deployment of smartcards with integrated biometrics for more effective identification

The most important way that this will happen will be to include end users, members of the operational community, throughout the design process in an iterative fashion. Researchers are used to working with other researchers and are largely unfamiliar with the responder community. Including first responders such as police officers, firefighters, paramedics and EMTs in the development process, and in future workshops, will help to bridge the gap between the two communities and keep researchers aware of the true needs of their clients. It will also expose the response community to cutting-edge technology, making them more familiar with its use and its possibilities.

4.2.1 Sociotechnical Systems

Technical and social factors interact to influence outcomes, and these outcomes can only be understood when social, psychological, environmental, and technological systems are assessed as a whole. This approach has become known as the sociotechnical systems perspective. It recognizes that organizations are made up of people (the social system), using tools, techniques and knowledge (the technical system) to produce services for clients (the external environment).

The effectiveness of the sociotechnical system depends on how well the social and technical systems are designed with respect to one another.

4.2.2 Living Laboratories

The rapid development of new technologies is creating a need for test environments where experimental applications could be prototyped, demonstrated, and tested under realistic conditions. Living laboratories bring together the designers and end users of technology to collaborate in its development. Real, experimental systems are deployed in real environments with evaluation by end users. What is needed is rapid prototyping cycles with users involved in each iteration of the system design. If technology is to solve practical, real-life problems, it must be tested during real-life activities that incorporate the behaviors, policy, and data that are likely to be encountered by the final system. One suggestion is to conduct the work in "Pasteur's Quadrant," an idea advanced by Donald Stokes (1997) to describe research that is equally focused on both the creation of new knowledge at its application.

4.2.3 Community-Based "Testbeds" Built on Existing Technologies

Incentive grants could be provided to groups of organizations to build trial demonstration programs in key metropolitan regions that are at high risk. The purpose of the grants would be to create local teams of technology experts and members of the response community who would work together to assemble and deploy emergency-response systems that are tested and evaluated for their effectiveness. One purpose of these centers would be training. By setting up a complete system, communities could stage whole-system training in which everyone who might be involved in responding to an unexpected event would do a walkthrough. This type of testing will serve to train end users, identify ways in which the system could be improved, and gain the trust of the community as the emergency procedures become more familiar.

Outreach activities should also be included to convey lessons learned from these exercises to other communities, particularly small and rural jurisdictions that have few resources for developing technology on their own. Outreach activities could also include sponsoring technology user groups, for first/initial responders, crisis managers, and system administrators.

4.2.4 Long-Term Commitment

Developing fundamentally new and improved systems for homeland security will require a long-term commitment. Designing for the next 3-5 years may simply result in patching fundamentally incorrect systems. A recent report by the National Research Council identified information-technology research opportunities for the support of homeland security that extend out ten years (Branscomb and Klausner, 2002). Improving the nation's ability to respond to unexpected events will require long-term funding commitments and the establishment of durable research and development centers with permanent staff to support the mission.

Recommendation 5: NSF should make long term investments in discovery based Living Labs as well as community testbeds 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 undertakes research in home-land defense. NSF should also accelerate the development of crisis management and visualization centers for decision support and extend access to local agencies as part of the community outreach activities.

5 Policy Issues

NSF should convene a large scale study or fund research whose focus is to uncover best practices learned by other entities, such as the Department of Defense, who have confronted and dealt with some aspects of the challenges of homeland security. Such a study on the use and impact of technology will help identify what practices can be readily transitioned from DoD to the state and local agencies and also identify the gaps that are unique to local and regional agencies. Military needs and imperatives, such as secrecy, are significantly different from those encountered in the civilian world, but these distinctions need to be carefully explored by policy experts.

Policy Issues

- NSF Should Study Best Practices
  - Many Of The Challenges Have Been Dealt With In DOD
  - Potential Tech Flow From DoD To State And Local
  - Military Not Same As Local Police
- Technology monitoring
- Cyberinfrastructure User Groups
  - Initial Responders
  - First Responders
  - Decision Coordinators
  - General Public
- Need For Integrated Team Approaches
  - Multi-disciplinary Centers
  - Virtual Multi-institutional Teams
- Provide mobile telemedicine / crisis management support for first responders
- Use and impact (social/organizational)
- Integrate the public into our distributed response infrastructure (e.g., ham radio operators for the 21st Century)
- Capture and reuse of the processes for learning/teaching, knowledge extraction, continuous improvement.

Part of this undertaking will involve the creation of new communities of responders, decision coordinators and the general public. How best can we help with the emergence of these communities? Does it help to form these communities based on the shared use of a prototype system? Who develops the prototype system? How do we balance off technology push with application pull based developments? Commercial interests can often pay for the development of demos and prototypes to showcase technical capabilities but financial support to uncover community needs may be harder to find but just as critical.

Early experiments in communities that lead to successful deployments of cyberinfrastructure systems for homeland security can serve as a model for other communities. Thus, it would be quite useful to understand the process by which such changes were introduced and absorbed within the participating entities.

Recommendation 6: NSF should invest in policy research to develop an understanding of what elements of cyberinfrastructure based systems developed for DoD applications can be readily transitioned into the civilian world and also uncover the unique gaps that remain to be filled. NSF should also play a lead role in facilitating a dialog among end users, technology providers and basic science researchers to identify the real needs of homeland defense and help develop a scientific agenda that can adequately serve the societal need.

6 Modality

Although securing the national defense has always been a part of its charter, only recently has a sense of urgency emerged for NSF to reengage and contribute more significantly to homeland security. Serendipitously, NSF has been funding cyberinfrastructure research for a number of years. Cyberinfrastructure activities, which have their roots in computational sciences, have evolved into a richer set of systems that have a very strong community focus. NSF programs and NSF funded cyberinfrastructure researchers have gradually built close working relationships with local responders as a way to test their algorithms against real data sets and validate their ideas in the context of the real word. Witness, for example, Prof. Chen's COPLINK system that helped snare Mohammad and Malvo, the alleged DC area snipers. So it seems that the shortest path from NSF's traditional activities to homeland security activities flows through the cyberinfrastructure in a technical and program management perspective.

Modality

- Accelerate the development of crisis management and visualization centers for decision support
- NOT Business as Usual for NSF nor It's Usual Research Community
- Scale
- Duration, Persistence
- Complexity (technical, managerial)
- Richness and Diversity of Partnerships
- Gaps, Chasms
- Approach (from linear to PQ model of research)
- Also more persistence and scale in provisioning of CI for the research community.
- Require local agency partnering as with education outreach

But, it will not be business as usual, either for the NSF or for its usual research community. Research in homeland security will require a greater commitment, both with regard to duration and persistence, from the scientific community and the agencies. The complexity of the partnerships that are likely to lead to breakthroughs will have to be richer and more diverse than usual.

Recommendation 7: NSF should recognize that home land defense is not a linear extension of other ongoing scientific research activities. NSF should make a long term, persistent commitment to fund home land defense research.

7 References

Boulis A., and Srivastava, M.B. (2002). *A Framework for Efficient and Programmable Sensor Network.* Paper presented at OPENARCH 2002, New York, New York. Retrieved from http://www.cens.ucla.edu/Project-Descriptions/SensorWare/index.htm on March 10, 2003.

Branscob, L., and Klausner, R., Eds. (2002). *Making the Nation Safer: The Role of Science and Technology in Countering Terrorism.* Washington, DC: National Academies Press.

Carpenter, B. (2003) *Grid Computing*. Internet Society. Retrieved from http://www.isoc.org/briefings/011/index.html on March 3, 2003.

CSTB (Computer Science and Telecommunications Board, National Academy of Science) (2002a) *Cybersecurity Today and Tomorrow: Pay Now or Pay Later*. Washington, DC: National Academies Press.

CSTB (Computer Science and Telecommunications Board, National Academy of Science) (2002b). *The Internet Under Crisis Conditions: Learning from September 11*. Washington, DC: National Academies Press.

FEMA (Federal Emergency Management Agency) (2003). A *Needs Assessment of the U.S. Fire Service*. Washington DC: Federal Emergency Management Administration. Retrieved from http://www.usfa.fema.gov/applications/publications on March 3, 2003.

Foster I., and Kesselman, C., Eds. (1999). *The Grid: Blueprint for a New Computing Infrastructure*. San Francisco: Morgan Kaufmann Publishers.

Huyk C.K., and Adams, B.J. (2002). *MCEER Special Report Series: Engineering and Organizational Issues Related to the World Trade Center Terrorist Attack. Vol. 3. Emergency Response in the Wake of the World Trade Center Attack: The Remote Sensing Perspective.* Buffalo NY: Multidisciplinary Center for Earthquake Engineering Research.

National Committee on Vital and Health Statistics, Workgroup on the National Health Information Infrastructure (2000). *Toward a National Health Information Infrastructure: Interim Report*. Retrieved from http://www.ncvhs.hhs.gov/NHII2kReport.htm on March 20, 2003.

Stokes, D.E. (1997) *Pasteur's Quadrant: Basic Science and Technological Innovation.* Washington DC: The Brookings Institution Press.

Putnam, Robert. *Bowling Alone* (2000), Simon and Schuster

8 Supplementary material

8.1 Workshop attendees

8.2 Workshop program

The agenda for the workshop is as follows:

Tuesday, February 25th
6:00 PM Reception
7:00 PM Dinner, Yigal Arens will summarize the report from the 2002 NSF Workshop -Responding to the Unexpected

Wednesday, February 26th
8:15 AM Continental Breakfast
9:00 AM Welcoming Remarks: Larry Smarr, Director Cal-(IT)2 and Prof. CSE Dept. Jacobs School of Engineering, UCSD
9:15 AM Opening Address: Peter Freeman, Assistant Director, Directorate for Computer & Information Science & Engineering
9:45 AM First Responder Perspectives
10:45 AM Break
11:00 AM Panel Discussion: Mobile Infrastructure
12:01 PM Lunch: Remarks by Frieder Seible, Interim Dean JSOE, UCSD and Esin Gulari, Acting Assistant Director, Directorate for Engineering, NSF
1:00 PM Panel Discussion: Fixed Infrastructure
2:00 PM Panel Discussion: Security

3:00 PM Break
3:30 PM Panel Discussion: Data/Grid
4:30 PM Panel Discussion: Collaboration and Decision Support
7:00 PM Dinner

Thursday, February 27th
8:15 AM Continental Breakfast
9:00 AM Breakout Work Sessions
11:00 AM Wrap-up Panel Discussion
12:30 PM Lunch