Decision Support in Disaster Management Based on Cyber-Infrastructure

Dr. Sohail Asghar

Shaheed Zulfikar Ali Bhutto Institute of Science and Technology, Islamabad Campus, Pakistan

Sohail.Asg@gmail.com

***Abstract**: The study of disaster management decision-making and its associated problems is an extremely significant area of concern which needs well-deserved attention from decision sciences research. This area of concern involves identification of the disaster management problem and suggesting an appropriate solution to address those issues and concerns in order to prevent and mitigate disasters. There are those who feel that handling of disaster management problems, challenges, threats and decision-making are extremely problematic. The obvious reason for this view point is that these problems and challenges are not satisfactorily resolved in the past. These problems include coordination, communication, data gathering and integration, dynamic monitoring of disasters, information sharing and analysis, along with collaboration and security issues. The question how to handle the uncertainties involved in such problems can be answered by implementing a cyber-infrastructure framework. Furthermore, such infrastructure can be used to make effective decisions for disaster management. The main objectives of this paper are as follows: (a) to identify the problems and challenges associated with disaster management; (b) to propose a cyber-infrastructure framework to address the currently facing problem, challenges of effective decision-making and threats in the disaster management domain.*

1. Introduction

The literature reveals that the subject infrastructure in general and cyber-infrastructure in particular is being defined in many different ways using different perceptive, and with different intentions in mind (NSF 2003; Berman and Brady 2005; Ramamurthy 2006). Nevertheless, we use cyber-infrastructure within the framework of disaster management in order to strengthen the disaster mitigation efforts and facilitate effective decision-making in a disastrous situation. The cyber-infrastructure may provide a basis that can help advance understanding and providing solutions for currently facing problems, challenges and threats and facilitates effective decision-making within a disaster management frame of reference.

The purpose of this paper is to propose a comprehensive framework of cyber-infrastructure by identifying its main components for enhancing a nation's capability to prevent disasters and reduce its vulnerability to disastrous incidents. The implementation of the proposed infrastructure will further help to make effective decision-making in disaster management.

The functionality of a cyber-infrastructure is an exceedingly complex task that requires coordination and communication among its different components and focused efforts from disaster mitigation agencies and stakeholders. Despite the tremendous amount of efforts being put to handle disaster and its aftermaths, yet, all the initiatives to prepare for a disaster cannot yield readiness. Readiness requires the use of all the procedure, polices, expertise, contingency plans and intelligent information systems under the umbrella of cyber-infrastructure.

In the light of today's threats of disasters, a critical cyber-infrastructure is an increasingly essential component for not only disaster mitigation measures but also to address currently facing problems in the domain of disaster management. Of utmost important is the core functionality of a cyber-infrastructure that

enables different agencies and authorities to communicate and disseminate information during the onset of a disaster. The need for improved cyber-infrastructure based solution towards disaster mitigation arises because of the following reasons:

1. In the aftermaths of September 11, bombing, it is clear that US government, business physicals and cyber-infrastructure are vulnerable to terrorists and cyber attacks (Hartman and Butler 2003). Therefore, improved assessment approaches for vulnerability are required.
2. A sophisticated cyber-infrastructure platform will allow a nation to strategize the ways to address disaster management issues.
3. To further upgrade the preparedness, response and recovery phases of disaster management by utilizing the capabilities of a new information technology based infrastructure.
4. In case of a disaster, the damage assessment is highly essential in order to gain assistance from different agencies. Such assessment can be made speedy with a help of technological based infrastructure to minimize the adverse affects of disaster and move on to the subsequent phases of response and recovery.
5. Disaster management is a challenging and multidisciplinary area with dynamic and changing needs. Because of this nature of the domain, there is an emerging need to solve its related issues. For instance, in case of a biological or chemical attack, there arises a dynamic need to forecast and continuous monitoring. In order to address this need, a complete set of on-line information and continuous monitoring of the disastrous event is required. In addition, such information is needed to be linked to other real-time data marts which may help in other activities such as evacuation planning. Therefore, based on these characteristics of the disaster management domain a highly sophisticated computational and communicational infrastructure is required.
6. We also emphasize the disaster management activities which include data collection and integration, data management, data mining and knowledge extraction, needs a well established cyber-infrastructure. Such infrastructure can be used for decision-making by disaster management experts, scientists, researchers, disaster management plans and policy-makers, and personnel's of different agencies and authorities.

Such an approach or methodology to develop cyber-infrastructure could focus on disaster management phases (preparedness, mitigation, response and recovery), security and planning. This alternative approach as compared to traditional methods would be more feasible, effective, efficient and acceptable (to different disaster management agencies). The need for the implementation of such infrastructure has become even more vital since 9/11 (Huyk and Adams 2002), Indian Ocean Tsunami, Hurricane Katrina and Earthquake in North of Pakistan. With the presence of more advanced forms of disasters such as cyber-terrorism, cyber-warfare, and bio-terrorism has raised the recognition and understanding of cyber-infrastructure. Furthermore, in case of a disastrous event, there are certain factors which could affect the normal systems such as mission critical information systems will be unavailable.

The structure of the paper is as follows: Section 2 discusses the problems, challenges and issues related to disaster management. Section 3 presents the overview of cyber-infrastructure and proposed a conceptual framework of cyber-infrastructure for disaster management. Section 4 explains how cyber-infrastructure can be used by a decision support system for decision-making. Section 5 uses an application scenario to illustrate such usage. Finally, Section 6 concludes the paper and sets the directions for future research.

2. Issues and Associated Problem in Disaster Management

Asghar, et al. (2006), proposed a comprehensive model for disaster management. The comprehensive model suggests that a large number of activities are involved in mitigating disasters. The involvement of this large number of activities raises the problem of complexity in disaster management. This section further elaborates on the issue of complexity that evolves from the management of such activities and

highlights the characteristics of a complex environment. The characteristics which make disaster management a complex domain are as follows:

- A large number of activities involved with varying features and functionality
- Changing environmental conditions
- A global perspective
- Uncertainty involved in decision-making
- Highly interdisciplinary and its changing nature
- Dynamic decision making is required
- Huge volume and scattered data at various sources
- The complexity of the system
- Dynamic monitoring is required
- Organizational collaboration, communication and coordination are cumbersome.

Because of the diversity and above-mentioned characteristics of the disaster management domain becomes complex. Another important question that has received attention in the past years in disaster management is how to use the distributed data and share the distributed resources in disaster management. In disaster management, it is a well established fact that a high-level of coordination among different agencies, authorities and organizations is required. Therefore, the flow of information is immense, and such information must be communicated between organizations and agencies in the event of a disaster. Hence, the need arises for an integrated communication platform. According to McEntire(2002) and Auf der Heide (1989), social and behavioural research indicates that coordination is a major challenge among individuals, groups and agencies that respond to disasters. Therefore, the ability to communicate, coordinate, collaborate and work effectively as a team can be a major factor in the success of any emergency plan. In response to these issues, we highlight the main problems associated with the development of disaster management systems. These are:

- establishing techniques for dynamic monitoring of disasters
- failure in maintaining communication links
- the slow access to data which makes for poor updating of disaster-related information
- difficulties in disaster-related data collection and integration
- poor communication and collaboration among agencies
- designing techniques for automated data processing from distributed sources
- designing and developing decision support system to help emergency managers achieve effective decision-making for different disaster management activities such as mitigation, preparedness, response and relief
- multiple models are required for decision-making and varying environmental affects which can significantly change the severity of a disaster.

Figure 1 shows the problems associated with disaster management. As mentioned earlier, such problems arise due to the complexity involved in managing a large number of activities.

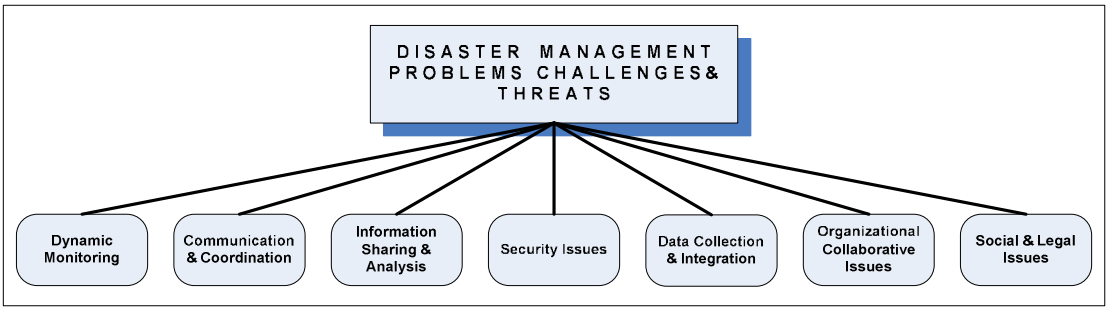

Figure 1: The overall Complexity of the Disaster Management Domain

Currently, there is large number of problems associated with disaster management which includes: dynamic monitoring, failure of communication links, slow access of data, data collection and integration,

information sharing and analysis, security issues, social and legal issues, automated data processing and communication and collaboration among different agencies, can be solved with the adaptation of a cyber-infrastructure. We are in an environment where disaster management actions (based on computational technology) are needed to address immediate problems, threats and challenges. A proposed model for cyber-infrastructure is provided in the next section.

3. A Cyber-Infrastructure Framework for Disaster Management

As mentioned in the previous section, disaster management is a challenging and complex area with dynamic needs and an adaptive nature (Schneid 2001). Cyber-infrastructure can potentially contribute towards meeting those needs and challenges because of characteristics attributed to the disaster management area such as a global perspective, dynamic decision support needs, the complex nature and huge volume of data scattered at multiple locations. This infrastructure helps to overcome the existing problems. With the implementation of this infrastructure we can solve the following problems: dynamic and the global monitoring of disasters, collection and integration of scattered data, communication and collaboration, global view of environmental changes and sharing decision-making for disaster management.

It is fact that there have been, and possibly will be, more problems encountered on the way to a new information forum. Quarantelli (1997) has insightfully investigated ten issues which may be problematic with the advent of these new technologies. In response to these problems, Fischer (1998) outlined several examples of how the new information technologies are being used, as well as how they may be used in the future, in a manner which may assuage several, though not all, of Quarantelli concerns.

"Cyber-infrastructure refers to the distributed computer, information and communication technologies that provide the platform on which to build the new types of scientific and engineering knowledge environments which will enable research to be conducted in new ways and with increased efficiency" (Hunter, Cook et al. 2004). The growing use of information, data, technology and sophisticated instruments is leading to the emerging concept of cyber-infrastructure , the objective of which is to provide an integrated, high-end system of computing, data facilities, connectivity, software, services and instruments that would enable all scientists and engineers to work in new ways on advanced research issues that would not otherwise be solvable (Blatecky 2003). Generally, the main components of a cyber-infrastructure could be:

- Communicational infrastructure
- Knowledge management systems, database systems and digital libraries
- Organizational structure and agencies involved
- Services and expertise
- Software, collaborative tools, equipments, advanced applications, algorithms and models and
- Computational, physical, technological and human resources.

The traditional question with respect to cyber-infrastructure is: what is Cyber-infrastructure, the answer to this question can be found in NFS Workshop (NSF 2003):

Cyber-infrastructure can be defined 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. Cyber-infrastructure 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.

"What is Cyber-infrastructure?"
–excerpted from Googlisms.com.

- cyber-infrastructure is the elimination of arbitrary limits on the scope and scale of research activity
- cyber-infrastructure is the linkage of computational and data resources with sensors and instruments
- cyber-infrastructure is a way to share data and tools in real time
- cyber-infrastructure is a network of knowledge
- cyber-infrastructure is revolutionizing earthquake engineering
- cyber-infrastructure is planning to recommend a substantial federal initiative in this area
- cyber-infrastructure is recommending major increases in the support for cyber-infrastructure
- cyber-infrastructure for disaster management is now available

The recent threats of man-made disasters such as terrorism and the current problems associated with disaster management, for instance global monitoring, communication, collaboration, and dynamic environmental changes, have reaffirmed the role of an emerging cyber-infrastructure to respond to these unexpected events and problems. The idea of the application of cyber-infrastructure to disaster management is relatively new and very limited research has been carried out in this area. Nevertheless, it is suggested in the research community that cyber-infrastructure might be used to support the unique needs of dealing with disasters and their disruptive consequences (NSF 2004). It is revealed that four applications of cyber-infrastructure address the needs critical to the disaster management domain.

- Ubiquitous vision and sensing.
- Syndromic surveillance.
- Information integration, sharing and visualization.
- Enabling the ecology of virtual organizations.

Therefore, based on the above-mentioned characteristics and challenges associated with disaster management we proposed model of cyber-infrastructure for disaster management. It is an attempt to support these application areas and to provide appropriate solutions to the current problems in the disaster management field. The model for cyber-infrastructure, (Figure 2), which focuses on the use of information sharing, integration and decision-making for agencies concerned with national security and disaster responses. It also assists the national security and disaster response agencies to develop consolidated decision making, data mining, coordination, collaboration and integrated information to adequately serve disaster needs. The main components of the cyber-infrastructure which is proposed in Figure 2 are:

- Communication and Coordination
- Information Sharing and Analysis
- Computational Technology
- Social and Legal Issues
- Organizational Collaborative Issues
- Cyber Security
- Data Gathering and Integration

The cyber-infrastructure model also explains the wide variety of information sources, organizations, resources, infrastructure and tools that become available due to its existence. It is now possible to make use of these when designing systems for disaster management. Making use of such information can provide a more global picture of the situation, which will result in the better management of disasters. This is especially relevant since the outcomes of man-made disasters (for example terrorism) can in some instances have similar components to natural disasters (for example a terrorist bomb blast may lead to fire spreading into a densely populated area). Therefore, the same or similar disaster management techniques may be relevant and useful. We outline the main advantages of making use of a cyber-infrastructure for disaster management as follows:

1. It makes use of more complete, distributed information and other resources in managing traditional disasters.
2. As globalization and advancements in technology have contributed to an increase in certain disasters (especially man-made such as terrorism) the same new technology can be used to counteract these disasters.
3. Cyber-infrastructure for disaster management systems facilitates the availability of relevant data for post-disaster lesson-learned analysis and for training purposes.
4. Cyber-infrastructure fulfils the need for coordination and communication and provides efficient, reliable and secure exchange and processing of desired information and data.

The infrastructure not only bridges the gap between traditional disaster management systems and emergent disaster needs but also helps to solve the problems encountered in the management of disasters. We emphasize and highlight the fact that the infrastructure is still not complete and new components can be incorporated as needed.

Therefore, the overall theme of the cyber-infrastructure is the need for integration, across technologies and across organizations (Berman and Brady 2005). The proposed framework synergistically combines on-going efforts for mitigating and recovery from different natures of disasters. Cyber-infrastructure is a newly emerging concept in technological based management system which provides reliable, robust, and efficient knowledge. We are using the concept of cyber-infrastructure within the framework of disaster management. The overall architecture of the cyber-infrastructure is depicted in Figure. Following are the typical characteristics of disaster management cyber infrastructure.

- Combines disaster monitoring, modeling, and decision-making in a seamless environment
- Address all the issues, phases and activities of disaster management lifecycle
- Gathers and integrate huge volume of scattered disaster data for all different kinds of disasters
- Employs modeling and simulation of disaster management processes
- Provides effective communication and coordination among different agencies and authorities
- Performs cyber security and information sharing and analysis
- Provides a global platform for disaster management trainings, exercises, and enforcing plans such as preparedness, mitigation, response and measure plans.

The advantages of the cyber-infrastructure designed for disaster management are:

- ❖ Bring together disparate functions, actions and plans that are developed and executed independently in the cyber-infrastructure arena.
- ❖ Maximize the use of scientific and computational technologies and minimize the use of paper information sharing.
- ❖ Support the implementation of advance operations and steps towards more effectively mitigating the effects of natural as well as man-made disasters.
- ❖ Ensure that comprehensive monitoring activities are developed and available through the use of such infrastructure for terrorist related and natural disasters.
- ❖ To further expand the development of information and action sharing capabilities required for the prevention, mitigation, response and recovery phases of a disaster.

- To provide a collaborative and well coordinated environment for the involvement of different agencies and authorities. Such infrastructure further narrows the gap and hurdles evolved from the coordination.
- Such infrastructure creates a novel system to better able to receive, analyze and process information and intelligence from various sectors.
- There are certain legal issues that may arise during the time of a disaster such infrastructure can be use as a tool to compare and seek guidance in order to solve the aroused legal issues.
- To utilize the skills and expertise of experts and intellectuals to prevent, deter, to respond to and recover from disasters.
- It provides an interface between different phases and activities of disaster management such as prevention, mitigation, response and recovery.
- The development of such infrastructure surely enables to set standards for communication and coordination.
- Implementation of such infrastructure establishes a platform for strategic directions, coordination, communication and continuous monitoring of preparedness and response activities of a disaster.
- Cyber-infrastructure creates a nation-wide global disaster communication network for the detection and surveillance by making use of the computational and technological infrastructures.
- It provides a shared collaborative working environment amongst disaster management agencies, institutions and jurisdictions to plan and prepare for contingencies. Such environment helps in further decision-making.

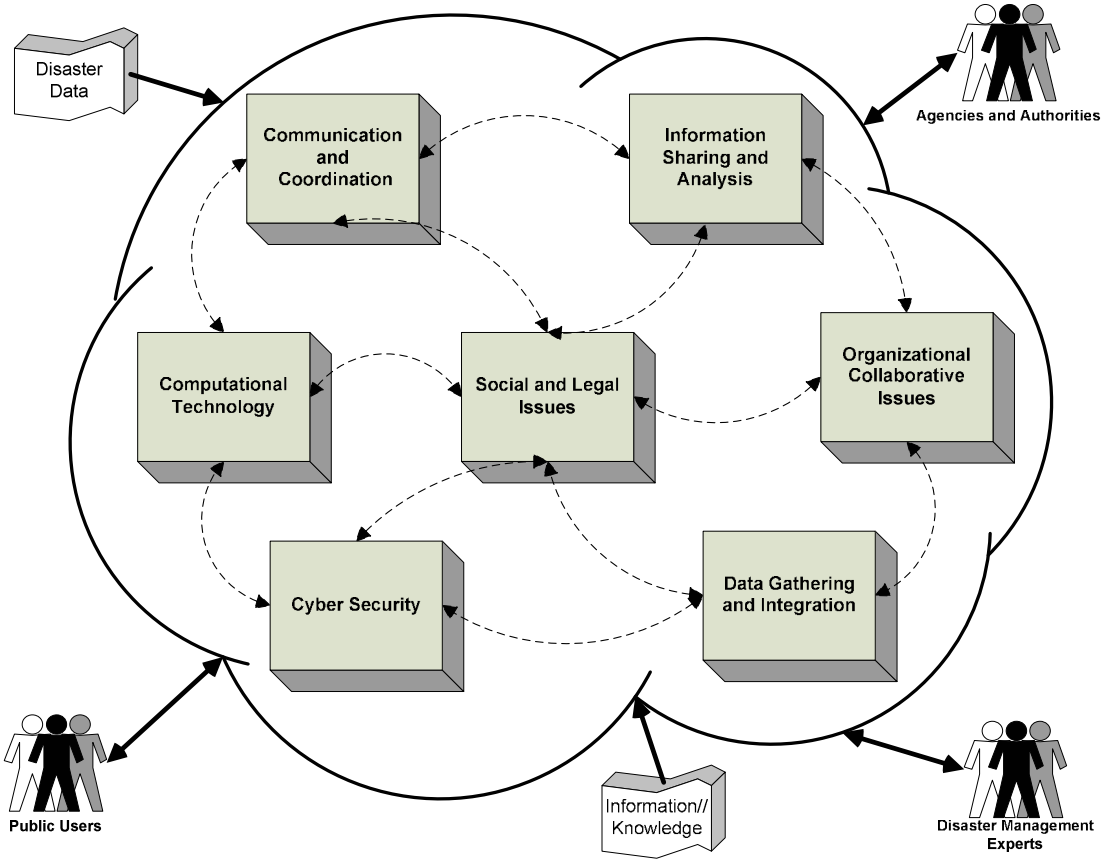

Figure 2: A Proposed Cyber-Infrastructure for Disaster Management

4. Decision Making on the Basis of Cyber-infrastructure

Decision-making is one of the most fundamental tasks that a manager has to perform. In disasters, bad decision-making has negative consequences. Therefore, the need for decision-making skills increases

significantly in disastrous situations (UNHCR 1990). In the last two decades, additional man-made disasters have emerged on top of existing ones, mainly due to globalization, inter-connected networks and the vast development in technology. The recent threats of these disasters have reaffirmed the urgency and importance of loss assessment and the need for decision support tools. Decision making on the basis of traditional approach has been unsuccessful, the reason behind this is the increasing number of catastrophes. Therefore, we have proposed a cyber-infrastructure (See Section 3) as a backbone for decision-making in disaster management. The traditional DSS models continue to work as normal with added advantages of cyber-infrastructure at the backend. This approach is shown in Figure 3. With the use of such infrastructure the decision-makers in the area of disaster management will get more effective and in-time decision to mitigate disasters.

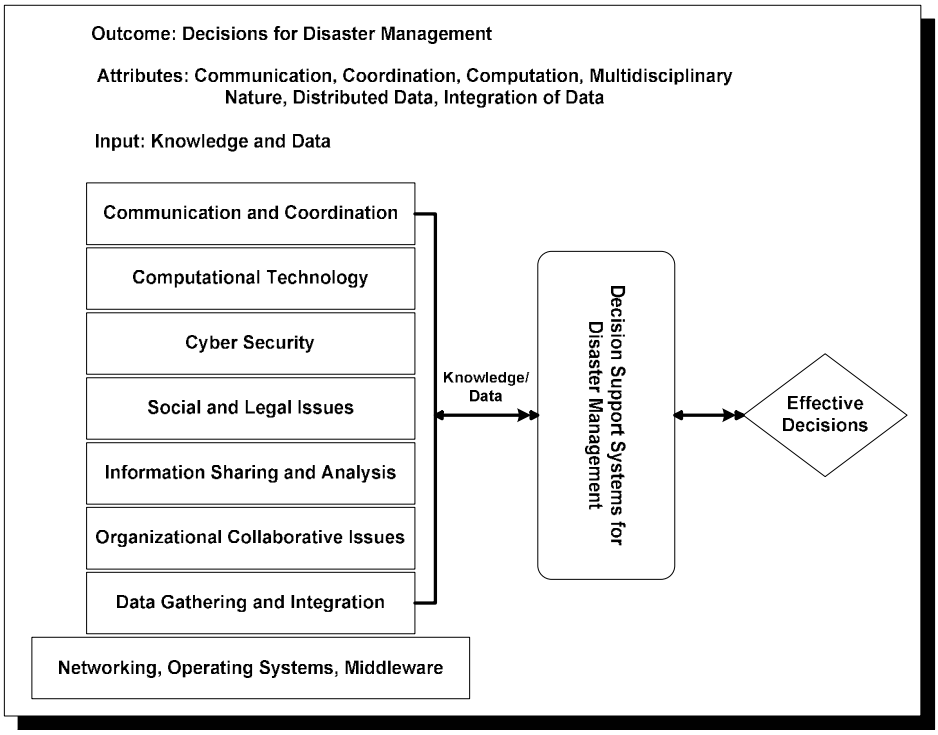

Figure 3: Cyber-infrastructure Enabled Decision-Making in Disaster Management

5. An Application Scenario

To highlight the significance of the decision-making in a disastrous situation on the basis of cyber-infrastructure, a scenario could be utilized. This approach allows us to derive the decisions from a given situation.

A Disaster Scenario: Pakistan Earthquake in 2005

A powerful 7.6 magnitude earthquake struck the India-Pakistan border with more than 140 aftershocks, causing extensive damage in Pakistan, India and Afghanistan. Reports indicate more than 82,000 people have been killed and more than 3.3 million people have been left injured or homeless. With more than 1,000 hospitals destroyed, the looming threat of illness, the need for decisive action in the face of this emergency was tremendous. However, financial, technological and computational support was needed to save lives and rebuild livelihoods! (Pak-Earthquake 2007).

The experts and decision makers may be interested in making a decision about the earthquake occurred and might need to access knowledge and other data sources to retrieve relevant information. Traditionally,

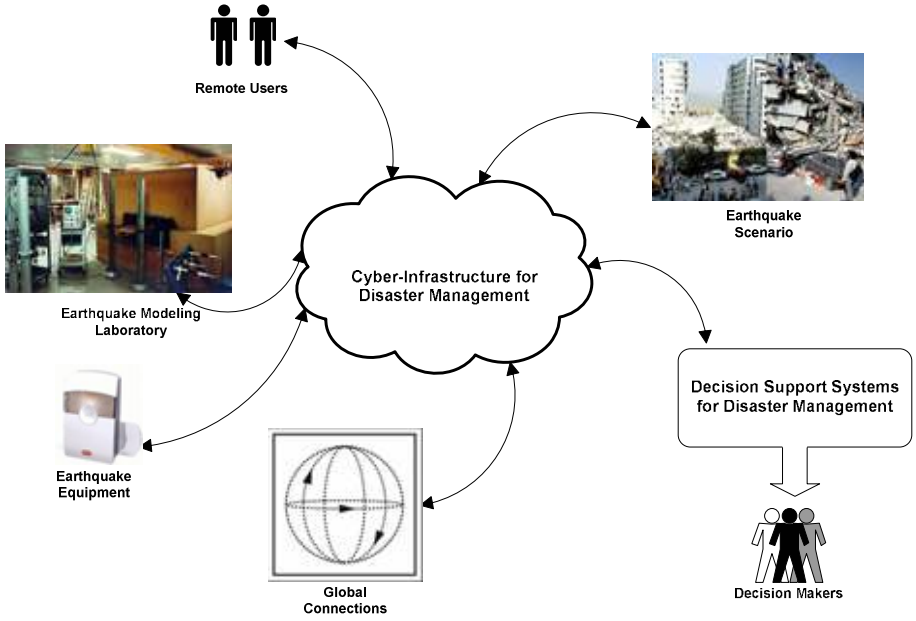

Figure 4: A Scenario of Decision-making in an Earthquake Disaster based on Cyber-Infrastructure

(without the presence of cyber-infrastructure) the decision support systems use existing models and data in reducing risk and selecting among alternatives. However, several problems have been identified with this approach:

- Distributed Resources, Models and Data – The resources, models and data required to make effective decisions will be geographically distributed across the Internet.
- Intelligent search for the appropriate models – Sometimes in case of a disaster for effective decision-making the DSS might reuse existing models (which might be remotely located). Without the presence of cyber-infrastructure such intelligent searching is a problem.
- Data Integration – Data integration is a complex problem in mitigating disasters.
- Lack of expertise – Even with the local expertise things becomes difficult to handle. However, experts located at a different site cannot supply the necessary expertise.

Figure 4 suggests a cyber-infrastructure based decision support system for decision-making in case of a disaster scenario (such as earthquake). The cyber-infrastructure by utilizing computational resources serves as a backbone of decision support systems. When an earthquake occurs, all the equipments, laboratories are connected to the cyber-infrastructure and feed the resources to a decision support system. Therefore, it provides on demand aggregation of computational resources (such as computational servers, instruments and sensors, databases, and data repositories) to decision support system at any time. Hence, a combination of recent technology trends and research advances make it feasible to connect cyber-infrastructure at the backend of a decision support system.

6. Conclusions and Future Research Directions

Nations are not safe from natural and man-made disasters despite the tremendous efforts put to mitigate disasters. The traditional ways are not sufficient enough to handle disasters. Therefore, new ways must be explored in order to mitigate disasters. On the basis of these facts this article has presented a comprehensive overview of many issues, problems, challenges and threats reshaping disaster management. In order to address these issues, a technological based cyber-infrastructure was proposed. Cyber-infrastructure can be defined as a layer between fundamental components and applications; a layer that empowers the federation of distributed resources. The purpose of this paper is to present a broader view of the disaster management problems and related issues, to address these issues and problems a cyber-infrastructure is proposed along with a discussion of its related components with implementation perspective. Recognizing the components of cyber-infrastructure is crucial towards any step taken to

further strengthen the infrastructure. Some significant and selected components of cyber-infrastructure discussed in this paper are:

- ✓ Communication and Coordination
- ✓ Information Sharing and Analysis
- ✓ Computational Technology
- ✓ Social and Legal Issues
- ✓ Organizational Collaborative Issues
- ✓ Cyber Security
- ✓ Data Gathering and Integration

In the context of disaster management, it is an era of an unprecedented data volume from diverse sources, multidisciplinary analysis and synthesis, integration of data, and knowledge-centered emphasis. The decision-making in such domain is extremely difficult and complex. In this paper, we have shown that if cyber-infrastructure has been used at the backend of a decision support system for disaster management it can facilitate effective decisions. In future we will report simulations and testing of this framework using the discussed scenario.

References:

1. Asghar S., Alahakoon D., et al. (2006). "A Comprehensive Conceptual Model for Disaster Management." Journal of Humanitarian Assistance: Published at the Department of Peace Studies, University of Bradford, UK, ISSN: 1360 - 0222, 1-15, July, 2006. http://www.jha.ac/. .
2. Auf der Heide, E. (1989). Disaster Response: Principles of Preparation and Coordination, C. V. Mosby Company, Toronto.
3. Berman, F. and H. Brady (2005). Final Report: NSF SBE-CISE Workshop on Cyberinfrastructure and the Social Sciences**:** Pages 1-50, available at www.sdsc.edu/sbe/.
4. Blatecky, A. (2003, Sep. 2004). "Cyberinfrastructure - Implications for Networks & Research." Retrieved Accessed: Sep. 2004., from Available: http://www.cenic.org/CENIC2003/presentations/Alan_Blatecky.pdf.
5. Fischer, H. W. (1998). "The Role of the New Information Technologies in Emergency Mitigation, Planning, Response and Recovery." Disaster Prevention and Management **7**(1): 28-37.
6. Hartman, J. L. and C. Butler (2003). Vulnerability Assessments: Communication Cannot be Overlooked. Proceeding of 2003 Association for Business Communication Annual Convention.
7. Hunter, J., R. Cook, et al. (2004, Accessed: Sept. 2004.). " E-Research Middleware: The Missing Link in Australia's Research Agenda." from Available: www.dstc.edu.au/publications/eReseachMiddleware.pdf.
8. Huyk, C. K. and B. J. Adams (2002). Emergency Response in the Wake of the World Trade Center Attack: The Remote Sensing Perspective, MCEER Special Report Series: Engineering and Organizational Issues Related to the World Trade Center Terrorist Attack. Vol. 3. Buffalo NY: Multidisciplinary Center for Earthquake Engineering Research. .
9. McEntire, D. (2002). "Coordinating multi-organizational responses to disaster: lessons from the March 28, 2000, Fort Worth tornado." Journal of Disaster Prevention and Management **11**(5): 369 - 379.
10. NSF (2003). Cyberinfrastructure Research for Homeland Security, NSF Workshop Report**:** February 25 to 27, 2003 in La Jolla, CA, Page(s) 1-28.
11. NSF. (2004, Accessed: Oct. 2004.). "NSF Workshop on Cyberinfrastructure Research for Homeland Security." from Available: http://dgrc.org/dgo2004/disc/posters/monposters/ph_rap.pdf.
12. Pak-Earthquake. (2007). Retrieved Jan. 2007, from http://www.pakquake2005.com/.
13. Quarantelli, E. L. (1997). "Problematical Aspects of the Information/Communication Revolution for Disaster Planning and Research: Ten Non-Technical Issues and Questions." Disaster Prevention and Management **6**(2): 94-106.
14. Ramamurthy, M. K. (2006). "A New Generation of Cyber-infrastructure and Data Services for Earth System Science Education and Research." Advances in Geosciences **8**: 69-78.
15. Schneid, D., Thomas, and Collins Larry (2001). Disaster Management and Preparedness. New York, Lewis Publisher, NY.
16. UNHCR (1990). An Introduction to Refugee emergency Management, EM 1 Training Module, 1st ed., UNHCR, Geneva.