Working Paper 99

What Hazards and Disasters are Likely in the 21st Century - or Sooner?[1]

Claire B. Rubin[2]

1998

As we enter the 21st century, we are facing new threats and risks, which may mean we will be dealing with new types of hazards and disasters. The disasters of the future may or may not be bigger or worse, but they are likely to be more complex and require more sophistication in response and recovery.

Some researchers and futurists have said that future disasters will result from increased technological dependence, urbanization, and social complexity. Some people are expecting new kinds and increasing numbers of technological accidents as well as events that were almost nonexistent in the past. For example, currently many countries are preparing to deal with the growing threats of chemical, biological, and nuclear accidents as well as the use of these agents as weapons of mass destruction. Another concern is with what international disaster officials call "complex disasters," which are events that have complex, humanitarian aspects - such as large, unplanned emigrations due to war. Disasters that involve both natural and technological hazard agents may be said to be *compound disasters*. Such events may entail sizeable humanitarian concerns as well.

As noted by Mitchell (1996), "Some of the most challenging industrial disasters of recent years have involved external hazards, such as extremes of natural and human conflict" - for example, the deliberate destruction of oil well facilities in Kuwait during 1992 Gulf War.

Obviously, the effects of disasters do not stop at plant gates. Furthermore, even with a decline or ending of industrial operations, hazards may be left behind in the form of dangerous wastes, ravaged environments, and moribund communities.

New Hazards and Threats

Some of the growing, emerging threats that we are likely to experience in the coming century are:

1. Events and conditions that exacerbate existing technological hazards;
2. Greater, more deadly impacts of natural hazards - including weather events;
3. Less confidence in and security for physical facilities, information systems, and databases;
4. Human error - intentional and unintentional;
5. Biological and chemical hazards, including:
    - Biotechnology hazards,
    - Marine toxins;
6. Terrorism;
7. Distant (international) sources of disasters.

1) Events and Conditions that Exacerbate Existing Technological Hazards

Technological advances - Advance in technology may reduce some hazards, but some add complexity to old threats, such as: fires in high-rise buildings, fires of hazardous materials (as in the interior of planes), and deliberate setting of oil well fires (as in Kuwait).

Massive Power Outages - In February of 1998, Auckland, New Zealand, (a city of about one million people) experienced the failure of four major power cables serving the central business district. Full restoration of power took several weeks, leaving the business and commercial communities scrambling for alternative ways to conduct business.

In the U.S., from July 2 to August 10, 1996, the Western States Utility Power Grid reported widespread power outages that affected millions of customers in several western states and adjacent areas of Canada and Mexico. These problems resulted from a variety of related causes, including sagging lines due to hot weather, flashovers from transmission lines to nearby trees, and incorrect relay settings. These problems in turn caused overloads in portions of the power grid, which caused voltage collapse and the tripping of transmission lines and generators.

According to the electric utility industry's trade association (EPRI), "The potential for such disturbances is expected to increase with the profound changes now sweeping the electric utility industry" (*Currents*, June 1997).

2) Greater, More Deadly Impacts of Natural Hazards - Including Weather Events

It can be expected that more vulnerable kinds of populations will be heavily impacted by known conditions. Large numbers of new retirement communities in the so-called Sun Belt of the U.S. have been built in areas with known hurricane hazards, tornado paths, or coastal storm risks. For example:

Hurricane Andrew (1992) in Dade County, FL - This storm affected numerous retirement communities, and was especially destructive of mobile home parks. It was the most expensive hurricane in the U.S. to date.

Urban Drought - Lack of water supply for fast growing residential areas in CA, AZ, and NV poses an increasing risk. Recently the book and educational TV series *The Cadillac Dessert* highlighted some of the great physical and political difficulties entailed in diverting the Colorado River for farm and urban uses.

3) Less Confidence in and Security of Physical Facilities, Information Systems, and Databases

As a result of the changes from dependence on industrial production to the new "Information Age," we are seeing the emergence of new kinds of technological accidents/disasters. Some examples include:

Telecommunications Failures - For example, we have experienced large-scale phone failures in recent years and have seen the resulting massive problems for businesses that cannot communicate. Major problems occur with the processing of credit card verification and payments, as well as with check clearing, etc.

Recently (May 20, 1998) a communications failure occurred that was the worst in 37 years of satellite service. Some major problems with the telecommunications satellite Galaxy IV drastically affected 120 companies in the paging industry. Additionally, radio and other forms of news broadcasts were affected. Although there are more than 200 communications satellites now orbiting the earth, including several dozen that serve the U.S., few people realize that most of the country's vastly expanding volume of paging messages are relayed around the country by a single satellite. "When it failed, close to 90% of the 45 million U.S. paging customers found themselves without service" (*Washington Post*, May 21, 1998).

The pager failure was doubly serious in that among the pager users were many emergency managers as well as medical personnel. Once again, an electronic service that people had been taking for granted failed totally and without warning. As noted in the *Washington Post*, "The outage adds to the fears that the world's communications infrastructure is more prone to massive failure than previously believed." (May 21; p. A22)

Computer Accidents or Sabotage - All sectors of society are now heavily dependent on computers. Lengthy power outages (such as the one in Auckland) could cause massive computer outages, with severe economic impacts - loss of sales, credit checking, banking transactions, ability to communicate and exchange information and data.

Computers/Communications/Telecommunications - Privacy, piracy, profits, progress, international boundaries;

public/private sector interactions and cooperation are a few of the many complex issues that must be dealt with with considering failure in these techological areas.

The President's Commission on Critical Infrastructure Protection (PCCIP) recently completed a report that addresses some of the "major vulnerabilities that exist in today's modern systems." The report says "There is increasing threat that the US could suffer something similar to an Electronic Pearl Harbor." The commission also offered proposals on training, building a planning and response infrastructure, and plans for further research and development.

Networked information systems present fundamentally new security challenges in addition to the benefits they offer. According to the PCCIP, "The development of the computer, and its . . . improvements, have ushered in the Information Age that affects almost all aspects of American commerce and society. Our security, economy, way of life, and perhaps even survival, are now dependent on the inter-related trio of electrical energy, communications, and computers."

The PCCIP report notes the following increased vulnerability: "Today, the right command sent over a network to a power generating station's control computer could be just as effective as a backpack full of explosives, and the perpetrator would be harder to identify and apprehend" (*President's Commission*, 1997, p. 3).

With the growth of a computer-literate population, increasingly numbers of people possess the skills necessary to attempt such an attack. "The resources necessary to conduct a cyber attack are now commonplace. A personal computer and a simple telephone connection of the Internet Service Provider anywhere in the world are enough to cause a great deal of harm" (*President's Commission*, 1997, p. 3).

A brief expanded list of the threats that we will be facing includes:

- blunders, errors, and omissions (see below) - incompetent, inquisitive, or unintentional human actions of omissions
- insider use of authorized access for unauthorized disruptive purposes
- recreational hackers - with or without hostile intent
- criminal activity - for financial gain, to steal information or services, organized crime
- industrial espionage
- terrorism - including various disruptive operations
- national intelligence - information warfare, intended disruption of military operations and/or of significant economic activity.

4) Human Error - Intentional and Unintentional

The Internet - As the Internet becomes more mature and more important, the loss of its services, whether by accident or intent, becomes a greater hardship for those relying on this new form of communication. "As more and more of the critical systems of advanced industrial society migrate to the Net, they become susceptible to new forms of sabotage, espionage, hacking and other mischief" (Gilder, 1997, p. 108.)

Intentional Internet Sabotage (cybernecine attack; cyber threats) - As suggested above, the outcomes of such activities may take the form of disruption of air traffic controls, train switches, banking transfers, police investigations, commercial transactions, policy investigations, personal information transfer, defense plans, power line controls, and other essential functions.

A chilling account of "information system terrorism," executed by young hackers whose main objective was mass disruption is provided by Jerrold Post and his colleagues (1998) in an article called "From Car Bombs to Logic Bombs: Weapons of Mass Destruction and Weapons of Mass Disruption."

In May 1998, in testimony to a Congressional Committee, six young men who were experienced "computer hackers" told committee members that they could bring the entire Internet to a crash in about 30 minutes. (*Washington Post*, May 19, 1998.)

Human Error - The "Millenium Bug" - Miscalculation or failure to think ahead has yielded the computer calendar dilemma called the Year 2000 (Y2K) Problem. Essentially, the problem is that much computer hardware and software contains chips and programs with calendars that recognize only the last two digits of the year - i.e., 19**98**. Hence, when the year 2000 arrives, the computers will recognize that year as 1900. Although this may sound like a simple or trivial problem, it is not. The implications are poorly understood, but potentially vast; and the work involved in rectifying this problem is daunting.

Thus, failure on the part of computer programmers to think a few decades ahead has led to the near-term crisis expected from hundred of thousands of computers that will not be able to function unless they are reprogrammed. This programming glitch has wide-ranging implications. Computer failures could affect emergency communications as well as routine civilian applications, such as telephone service, brokerage transactions, credit card payments, Social Security payments, mortgage payments, pharmacy transactions, airline schedules, etc.

Computer Viruses - In contrast to the Y2K problem, computer viruses are an intentional hazard. Viruses can cause a variety of computer and network problems. It was recently noted that there now are more than 2,000 such viruses (*Contingency Planning and Management*, 1998). One of the unfortunate side effects of these misguided human efforts is the huge loss of productive time on the part of programmers and managers - time that could be spent on creative new endeavors, instead of on remedial actions.

5) Biological and Chemical Hazards

Medical Waste Products - We have already seen some examples of the mishandling and improper disposal or storage of medical wastes and low-level radioactive products from medical use. A few years ago an incident occurred in New Jersey when improper disposal of medical wastes resulted in some of the used products ending up on Atlantic Ocean beaches.

Food Processing By-Products - A recent example of a biotechnological incident occurred in the state of Virginia. There, environmentalists have charged that the state is not doing enough to protect the public water supply from waste products from numerous chicken processing plants. Pollutants are entering the Potomac River, where they are alleged to be causing disease among fish and may have an affected drinking water downstream.

Contaminated Food - Recently, millions of pounds of possibly contaminated beef from the Hudson packing plant were seized by the Department of Agriculture and destroyed.

Hardly a week goes by in the U.S. without a story in the newspaper about an E-coli or botulism breakout. Usually, these are small, limited events.

Marine Toxins - Pfeisteria is a recently identified phenomenon in Maryland, Virginia, and North Carolina. It is not yet know if it occurs naturally, or is human-induced due to farm waste. It is an innocent organism that can turn toxic in 24 hours. Its effects on marine life and on humans who come in external contact with it or ingest it are not yet known. However, according to one Woods Hole scientist, "The issue of marine toxins and human health is a huge, but barely recognized, one in the U.S." [*Washington Post* 9/18/97].

6) Terrorism

As already suggested, terrorism may take many forms; it can involve not only convention weapons, such as guns and bombs, but also chemical, biological, radiological, and nuclear weapons. Terrorism may take the form of destruction of infrastructure (as in the New York Trade Center bombing) and/or harming or killing large numbers of people (as in the Oklahoma City federal office building bombing). It may also take the form of a protracted series of incidents, such as the murders perpetrated by the so-called Unabomber in the U.S. over a period of almost 20 years.

New efforts by the emergency management and the law enforcement communities are needed, so that they can learn to work cooperatively to detect, deter, and counter such terrorist incidents.

7) Distant (International) Sources of Disasters

Increasingly, localities will face disastrous conditions created by sources quite distant - possibly even from another country - the circumstances being beyond the control of U.S. emergency managers. Perhaps the most serious example in recent years was the Chernoby nuclear disaster. In that event, several European countries experienced increased radiation levels as a result when the reactor exploded in Russia.

As another example, at the time this paper was being prepared (May 1998), a large number of wildfires burning out of control in Mexico and Central American are causing serious smoke visibility and health problems for American citizens in Texas and other southwestern states.

Again, clearly the societal risks and vulnerabilities in our modern industrial world are growing rapidly. Both natural and technological disaster agents endanger larger and more complex populations and systems, and they can have increasingly severe effects; more vulnerable kinds of populations will be affected than in the past; and growing metropolitan areas are particularly at risk, although many are not well prepared to cope with disasters.

As events grow larger or cross national boundaries, international organizational arrangements will be needed to prepare for and respond to threatened or actual disasters.

THE CHALLENGE OF ANTICIPATING CHANGE AND DEALING WITH IT

What Organizational and Institutional Steps Are Needed?

How will we (those responsible for emergency management) function in the future? How can we complement and supplement what achievements and effective processes and procedures we now use in order to prepare for the risks, threats, and accidents in the next century?

Organizational Arrangements

Emergency management agencies and personnel will have to get away from the "stovepipe" mode of organization into broader operating frameworks. We will need to integrate the main types of hazards (natural, technological, and others) into a more comprehensive approach and organizational mode. The organizational forms, the partnerships created (whether ad hoc or more permanent), the means of communication, and the information intake and decision-making processes all are evolving. A few examples follow:

Public and Private Efforts: Cooperation, Coordination, Partnerships
In Eastern Europe, where the public sector formerly owned all of the industry - including those that were major polluters - there are major efforts underway to improve emergency planning and management capability and to use both public and private expenditures for those efforts. In the U.S., public and private partnerships are being forged at a rapid rate. For example the property and casualty insurance industry has been working with a broad array of public and nonprofit organizations, engaging in joint efforts to reduce loss of life and property from major natural disasters.

Working Relationships
Among the important aspects of multidisciplinary and multiorganizational efforts are the need for teamwork, sharing, and trust. Compounding this problem, many new players have entered the arena (such as law enforcement officials). New accommodations must be made and also appreciation is needed for the fact that new players mean new perspectives and expertise.

New Equipment and New Ways and Means of Working
The telecommunications area is obviously advancing at amazing speed; acquiring new equipment and teaching emergency workers in the field to use it effectively and appropriately are highly demanding, but important tasks.

Again, use of the Internet in disasters is growing by leaps and bounds. Recent events, such as the Kobe Earthquake in 1995 and the Midwest Floods of 1997, have involved extensive use of the Internet to communicate text and pictures of the events, almost in real time.

For example, during the Red River flood in May 1997, through the Internet responders and researchers who were not locally based were able to see pictures of the flooding, read local newspaper headlines (from the *Grand Forks Herald*, whose office building was destroyed but nonetheless published a Web-based daily paper), and access situation reports from state and federal emergency management agencies.

Building on Existing National Response Plans and Experience
There are several national response plans. The best-known, because it is has been used to deal with natural disasters, is the Federal Response Plan (FRP). The FRP was an outgrowth of federal efforts to plan for a catastrophic earthquake, but it has since been extended to deal with urban fires and riots, and was used to respond to the Oklahoma City bombing. Most recently, the FRP was extended for use in the event of a terrorist attack, including incidents involving nuclear, biological, and chemical agents, as well as weapons of mass destruction.

As the FRP is expanded to include more types of hazards, it will be necessary to recognize the broader array of specialties needed to deal with these risks and to draw upon the expertise of many more individuals and organizations. For example, law enforcement experts will be working side by side with emergency management specialists in future federal responses.

NEW THINKING IS NEEDED ON THE PART OF PUBLIC, PRIVATE, AND CIVIC LEADERS

In a recent book, Mitchell (1996) makes the point that the record of human response to large-scale industrial disasters is disquieting. He argues for more empirical research, more comprehensive thinking, and notes the need for institutional reforms and innovations in order to improve both response and recovery.

More specifically, some of the new needs are:

- **Broader thinking**
  - multidisciplinary
  - multihazard
  - multiinstitutional
  - international cooperation

  At the federal level, agencies tend to operate "stovepipe," narrowly focused programs, and in academic institutions, the approach to problem solving often is by single discipline. These approaches are no longer appropriate for the problems we face in the coming century.

  It is worth noting that the sponsor of the Fifth Annual Conference of the International Emergency Management Society (TIEMS), the Institute for Crisis and Risk Management at The George Washington University is, in fact, a new interdisciplinary center, engaged in research and teaching.

- **Joint planning and sharing of resources - among regions, states and nations**
  - mutual planning and mutual aid for response
  - xample: regional earthquake consortia in the U.S.

- **Regional and bilateral organizational arrangements**
  - Example: US/Canada/Mexico, US/Japan agreements

- **More research, especially empirical case studies**
  - examples of technological hazards triggered by large-scale natural disasters
  - case studies of what works and what does not (policies, programs, organizational arrangements)

- examples of the most cost-effective ways to deal with hazards/disasters (which mitigative measures are the most cost-effective and why)
- collaboration with the research communities studying environmental monitoring efforts, risk assessment and risk management techniques, economic analyses, behavioral studies

- **More and better risk assessment and risk management efforts**

- **More training**
  - in substantive areas of emergency management
  - in telecommunications techniques, use of computers, Internet and Intranet use, Web page development and use

To close, I quote Attorney General Janet Reno, who recently was interviewed by a reporter from *Government Technology* (May 1998). She said, "Technology should serve society, not rule it," and, finally, "Technology should promote public safety not defeat it."

REFERENCES

Contingency Planning and Management, May 1998, p. 34.

Gilder, George, "Inventing the Internet Again." *Forbes ASAP*, June 2, 1997.

"Last Year's Western Power Outages Explained." *Currents*, June 1997.

Mitchell, James K. 1996. *The Long Road to Recovery: Community Responses to Industrial Disaster*. New York: UN University Press.

Post, Jerrold; Eric Shaw, and Keven Ruby, Keven. 1998. "From Car Bombs to Logic Bombs: Weapons of Mass Destruction, Weapons of Mass Disruption," pp. 591-604 in the *Proceedings of The International Emergency Management Society (TIEMS), Fifth Annual Conference, May 19-22, 1998, Washington, D.C.* Washington, D.C.: The George Washington University, Institute of Crisis and Risk Management.

President's Commission on Critical Infrastructure Protection. 1997. *Summary Report: Critical Foundations; Thinking Differently*. Available via the World Wide Web at: <http://www.pccip.gov>.

Quarantelli, E.R. 1992. "Urban Vulnerability and Technological Hazards in Developing Societies." Article #236. Newark, Delaware: University of Delaware, Disaster Research Center.

_____. 1993. "Environmental Disasters Will be More and Worse but the Prospect is Not Hopeless." Article #250. Newark, Delaware: University of Delaware, Disaster Research Center.

_____. 1996. "The Future Is Not the Past Repeated: Projecting Disasters in the 21st Century from Present Trends.: Article #298. Newark, Delaware: University of Delaware, Disaster Research Center.

Reisner, Marc. 1996. *Cadillac Dessert: The American West and Its Disappearing Water*. New York: Penguin Press.

"Research Priorities for the 21st Century." *Environmental Science and Technology*, January, 1997.

Washington Post, September 18, 1997.

_____,"How Much Technology is Too Much?" October 6, 1997.

_____ May 19, 1998.

_____ May 21, 1998, p. 1, 22 ff.

NOTES

1. This paper is based on an earlier paper, "New Hazards/Disasters in the Coming Century," pages 237-243 in the *Proceedings of the International Emergency Management Society (TIEMS), Fifth Annual Conference, May 19-22, 1998, Washington, D.C.* published by the George Washington University, Institute of Crisis, Disaster, and Risk Management, May 1998; pp. 237-243.

2. Principal of Claire B. Rubin & Associates, Disaster Research and Consulting, P.O. Box 2208, Arlington, VA 22202; tel: (703) 920-7176; fax: (703) 892-7082; e-mail: cbrubin@aol.com.

July 8, 1998