

SAND98-2289  
Unlimited Release  
Printed October 1998

# **Modeling Requirements for Simulating the Effects of Extreme Acts of Terrorism: A White Paper**

R. J. Pryor, D. Marozas, M. Allen, O. Paananen,  
K. Hiebert-Dodd, and R.K. Reinert

Program Management Department  
Sandia National Laboratories  
Box 5800  
Albuquerque, NM 87185-0619

## **Abstract**

This white paper presents the initial requirements for developing a new computer model for simulating the effects of extreme acts of terrorism in the United States. General characteristics of the model are proposed and the level of effort to prepare a complete written description of the model, prior to coding, is detailed. The model would simulate the decision processes and interactions of complex U. S. systems engaged in responding to and recovering from four types of terrorist incidents. The incident scenarios span the space of extreme acts of terrorism that have the potential to affect not only the impacted area, but also the entire nation. The model would be useful to decision-makers in assessing and analyzing the vulnerability of the nation's complex infrastructures, in prioritizing resources to reduce risk, and in planning strategies for immediate response and for subsequent recovery from terrorist incidents.

Intentionally Left Blank

## Contents

Introduction.....	5
Scope.....	6
About the Panel .....	6
Overview of the Proposed Model.....	7
Threat Scenarios.....	8
Scenario 1: Information Warfare .....	8
Scenario 2: Electric System Failure.....	9
Scenario 3: Biological Warfare.....	9
Scenario 4: Nuclear Warfare .....	10
Actors in the Model.....	10
Simulation Output .....	11
Output Types.....	11
Output Time Frames .....	12
Agent-Based Approach .....	12
Model Development Requirements.....	13
Modeling Needs for Actors .....	13
Federal Emergency Management Agency (FEMA).....	13
Federal Reserve.....	14
Banking and Financial Investment Systems.....	14
Households .....	14
Medical Systems.....	15
National Guard.....	15
Industries/Firms.....	15
Federal Government.....	16
Telecommunications Systems.....	16
Transportation Systems .....	17
Electric Power Systems .....	17
State and Local Organizations.....	18
Life-Support Systems.....	18
Proposed Level of Effort (LOE).....	19

Summary and Future Directions..... 20  
References..... 21

**Figure**

Figure 1. Top-level Model Features..... 7

**Tables**

Table 1. Actors and Scenarios ..... 11  
Table 2. Model Documentation Requirements..... 19

# Introduction

On August 7, 1998, the world was once again rocked by violent acts of terrorism, when bombs went off simultaneously at U.S. embassies in Kenya and Tanzania. In Nairobi, Kenya, where 254 people were killed, the magnitude of the disaster overwhelmed local emergency services, police, and the city's seven hospitals [1,2]. The hospitals treated more than 4700 injured people—many who were unconscious and in shock [2,3]. And the hospitals' basic medical needs were extensive: there were shortages of syringes, needles, bandages, x-ray film, blood, pain killers, and antibiotics [4].

Officials in Kenya made urgent requests to the international community for medical supplies, rescue equipment, and specialized personnel. However, because of Nairobi's location, it would take at least a day for help to begin arriving from the United States, Israel, South Africa, and other countries. Within the first 24 hours, then, what the community had on-hand and how the responsible agencies marshaled these resources amidst widespread confusion and panic had significant social impacts. It was the difference between life and death for some. For others, it meant immediate treatment or prolonged suffering. There were several accounts of citizens voluntarily taking victims to hospitals in their own cars and helping in the search operations.

Nairobi's reaction to the bombing is not unlike that of other communities struck by terrorist acts, or even natural disasters. Emergency plans are activated as a first response to the immediate needs of the affected population. Numerous organizations, public and private, are involved, requiring immense efforts at coordination and cooperation. Depending on the type and severity of the incident, these organizations may have to deal with a myriad of problems—ones that can extend far beyond the area of the disaster and require personnel, equipment, and supplies from outside that area as well. Prolonged disruptions in critical services (e.g., phone, electricity, and transportation) and shortages of critical resources like water and food can place great strains on subsequent recovery efforts and result in significant economic and social costs not only to the targeted area but to an entire nation.

Since the bombing of the New York World Trade Center and the attack on the Murrah Federal Building in Oklahoma City, the U.S. government has focused significant attention and resources on enhancing the nation's ability to respond to acts of international and domestic terrorism on U.S. soil. Several examples illustrate this thrust:

- The Nunn-Lugar-Domenici Domestic Preparedness Program, implemented by the Department of Defense, is targeted toward improving the capabilities of state and local emergency response agencies to prevent and respond to terrorist incidents involving weapons of mass destruction [5, 6].
- Joint Terrorism Task Forces have been established in 16 cities across the United States. These task forces are staffed by FBI agents and federal, state and local law enforcement officers [7, 8].

- In 1996, the President's Commission on Critical Infrastructure Protection was established to assess the nation's vulnerabilities in critical services (infrastructures) and recommend remedial actions. Eight critical infrastructures were identified: transportation, oil and gas production and storage, water supply, emergency services, government services, banking and finance, electrical power, and information and communications. The Commission published its final report, *Critical Foundations*, in 1997 [9].
- In 1998, Presidential Directive 63 established several governmental mechanisms which included the Critical Infrastructure Assurance Office (CIAO) in the Department of Commerce and the National Infrastructure Protection Center (NIPC) at the FBI. The CIAO will facilitate the creation of a national plan to protect the nation's infrastructures [10]. The mission of the NIPC is "to detect, deter, assess, warn of, respond to, and investigate computer intrusions and unlawful acts, both physical and 'cyber,' that threaten or target our critical infrastructures" [11]. Also in 1998, President Clinton appointed the first National Coordinator for Security, Infrastructure Protection, and Counter-terrorism [12].

## Scope

The President's Commission on Critical Infrastructure Protection recommended that the federal government increase its research and development (R&D) investment for infrastructure assurance [9]. In this paper, we are advocating the development of a new computer model for simulating the effects of extreme acts of terrorism in the United States. This model would specifically address three of the six R&D areas identified by the Commission: 1) *Vulnerability Assessment and Systems Analysis* to identify critical nodes within infrastructures, examine interdependencies, and help understand the behavior of these complex systems; 2) *Risk Management Decision Support* to help government and private sector decision-makers in prioritizing the use of finite resources to reduce risk; and 3) *Incidence Response and Recovery* to assist decision-makers in planning a coordinated strategy for immediate response and for subsequent recovery from terrorist incidents.

The initial requirements for the new computer model were identified during a panel discussion of scientists at Sandia National Laboratories (Sandia) on July 16, 1998. This paper describes the general characteristics of the proposed model and defines the level of effort (LOE) necessary to develop a complete written description of the entire model, prior to software coding.

## About the Panel

The panel was composed of six members. Dr. Richard Pryor, who organized the panel, is a computational physicist with extensive experience in agent-based modeling. Dr. Dianne Marozas, a Principal Member of the Technical Staff in Sandia's Infrastructure Surety Department, is working on the development of agent-based models of critical

infrastructure systems. Dr. Mark Allen, an economist, has just returned to Sandia after an eighteen-month assignment at the CIA. Dr. Orman Paananen, also an economist, has developed a variety of microeconomic and regional economic models. Dr. Kathie Hiebert-Dodd is a mathematician who currently manages programs in information management and information technology. Ms. Rhonda Reinert is a family studies specialist.

## Overview of the Proposed Model

This section provides a high-level description of the computer model envisioned by the panel. The model would simulate the decision processes and interactions of complex U.S. systems (or actors) engaged in responding to and recovering from a particular terrorist incident. The actors include the infrastructures identified by the President’s Commission on Critical Infrastructure Protection and other systems deemed critical by the panel. Four different scenarios would be treated. These scenarios span the space of extreme acts of terrorism that have the potential to affect not only the impacted area but also the entire nation. They cover information warfare, electric system failure, biological warfare, and nuclear warfare. For each simulation, the computer model would calculate the effects of the terrorist incident in terms of social impacts, economic costs, and organizational effectiveness for the first 24 hours and for the first 30 days.

Figure 1 shows the top-level model features. The subsections following give a preview of the threat scenarios, the actors in the scenarios, the simulation output, and the modeling approach.

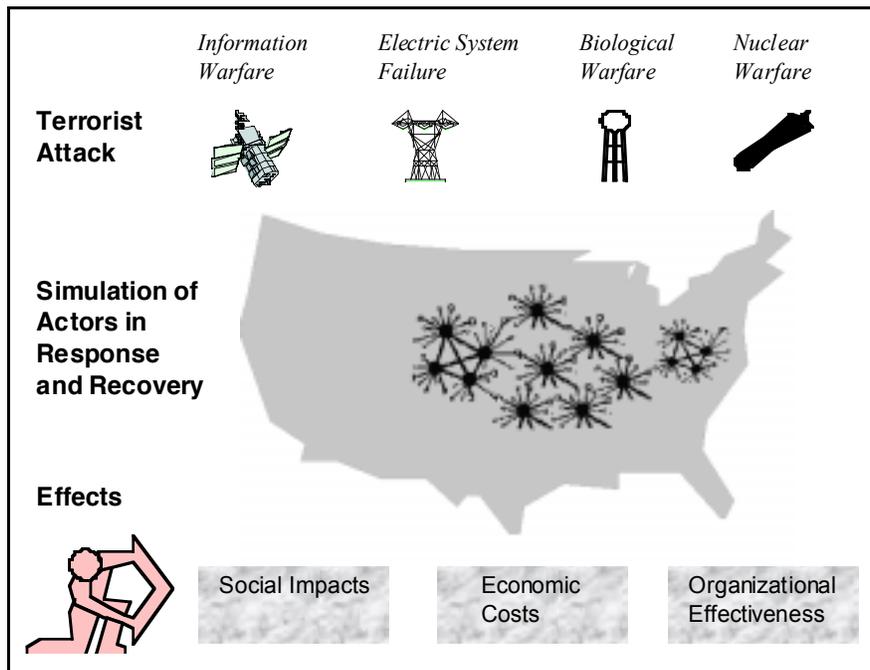


Figure 1. Top-level Model Features

## Threat Scenarios

The four threat scenarios being considered are beyond the scope of terrorist acts that have occurred in the United States. In brief, the threat scenarios cover the following types of incidents:

- ◆ Scenario 1: Information Warfare – Destruction of several communications satellite systems serving the United States
- ◆ Scenario 2: Electric System Failure – Attack on an electric system supplying power to a major U.S. region
- ◆ Scenario 3: Biological Warfare – Contamination of the water supply system of a major U.S. city
- ◆ Scenario 4: Nuclear Warfare – Small-scale nuclear detonation in a major U.S. city

These scenarios have been selected because they represent a range of events that would have resounding effects throughout the country and would require the interplay and coordination of numerous decision-makers and resources to assist in response and recovery efforts. Because of the complex interdependencies of the systems within our nation, and globally as well, it is understood that any one of these terrorist acts could trigger significant disruptions in other systems, whose behavior also would be modeled, both temporally and logically.

There is a notable and intentional difference in coverage area and severity across the scenarios. The telecommunications and electric power scenarios (1 and 2) would potentially impact a larger number of people than the biological and nuclear scenarios (3 and 4), while the effects of scenarios 3 and 4 would incur far more human suffering.

In the paragraphs that follow, we have provided brief sketches of four possible scenarios. Developing detailed scenario specifications is part of the LOE estimate for this project. Additionally, each sketch includes one or more sample incidents that have occurred nationally or internationally. These incidents, arguably minimal relative to the actual scenarios and not all terrorist-initiated, are presented to illustrate some of the consequences that have accrued from real-life events experienced during this decade.

### **Scenario 1: Information Warfare**

This scenario focuses on a telecommunications outage caused by the destruction of several major satellite systems. Services to 100 percent of the impacted users in the affected areas would be completely out for three to five days. By 15 days, most of the services would be restored. Satellite systems that might be targeted as part of this scenario include the Global Positioning System (GPS) operated by the U.S. Department

of Defense and various communications satellites that provide video and television broadcast services and Just-in-Time capabilities.

Prior to May 1998, most people probably did not know and probably could not even imagine the impact that one satellite could have on a country. Galaxy 4 provided a wake-up call, as this five-year-old satellite serving the United States and the Caribbean lost its bearings and began rotating [13, 14]. Galaxy's failure, the first since communication satellites entered service, knocked out almost 90 percent of the pagers used in the United States, thousands of television systems and television state broadcasts, and retail point-of-sale networks [13, 15]. Most paging services were restored within three days [15, 16].

### **Scenario 2: Electric System Failure**

In this scenario terrorists attack an electric system that supplies power to a major region in the United States. As a result, 100 percent of the electric power to customers is lost for 20 days.

Last year, San Francisco experienced a taste of what life might be like under such a scenario, albeit for a small amount of time. At 6:15 a.m. on October 23, 1997, someone flipped the switches in the Mission Street substation, which is the heart of the city's power distribution system. Power to 126,000 customers of Pacific Gas and Electric was knocked out for three and one-half hours, commuter traffic was disrupted, and municipal railways stopped working [17, 18].

A more poignant case for observing the impact of a major electric crisis is that of Auckland, New Zealand earlier this year. Failures of four power cables on February 20, 1998 effectively left the central business district (CBD) without power [14, 19]. There are differing accounts of the actual length of the power crisis, ranging from five and one-half weeks to nearly ten weeks [20, 21]. Mercury Energy, the supplier of electricity to Auckland, brought in a number of large generators from Australia to relieve some of the pressure of restoring power to the CBD [22]. The impact on commerce and inner-city life was significant during the crisis: some businesses moved their operations to the suburbs, as did universities and colleges; some businesses plunged into financial peril; and thousands of hotel guests and residents of the CBD moved [21, 23]. Shops that remained open in the city operated on rationed power or with noisy diesel-fuel generators [21].

### **Scenario 3: Biological Warfare**

Biological, chemical, and radiological threats are gaining increased attention, according to the President's Commission on Critical Infrastructure Protection. A national laboratory that performed work for the Commission found that biological and chemical agents pose a credible threat to the nation's water supply system [9]. In this scenario, the water supply system of a major U.S city is contaminated by a biological weapon. As a result, 30 percent of the people would be sick for approximately 15 days.

Though such a crisis may seem alien to U.S. citizens, it is not inconceivable. In 1995, Japan experienced its worst terrorist attack in modern times. Using sarin gas (a chemical agent), members of the Aum Shinri Kyo cult attacked the Tokyo subways. Twelve people were killed in the incident, and more than 5,500 were sickened [24] The cult was also pursuing a sizable biological warfare capability [25].

#### **Scenario 4: Nuclear Warfare**

This scenario is the most severe of the four. There is a small-scale nuclear detonation in a major U.S. city. The consequences are devastating: 2,000,000 people are killed. While the magnitude of such an event seems overwhelming, it is a scenario that the panel thought should be considered.

Speaking before a conference on proliferation issues sponsored by Los Alamos National Laboratories in 1996, Dr. John M. Deutch [26], Director of the Central Intelligence Agency, expressed his belief that nuclear weapons are the least likely choice of the weapons of mass destruction for terrorists. However, Dr. Deutch also pointed out that nuclear materials and nuclear technologies are more accessible today than they have ever been before—as a result of the breakup of the former Soviet Union and deterioration of control over its nuclear weapons establishment.

Several major acts of terrorism on U.S. soil in the 1990s have made the possibility of a more devastating incident imaginable to many citizens. In 1993, an approximately 1200-pound urea nitrate bomb was detonated in a van in the parking garage of the World Trade Center in New York. Six people were killed and more than 1000 people were injured [27]. The property damage was estimated at over half a billion dollars [8]. In 1995, an improvised explosive device placed in a rental truck destroyed the Alfred P. Murrah Federal Building in Oklahoma City. One hundred sixty eight people were killed and hundreds of others were wounded. The property damage for this incident was assessed in the hundreds of millions of dollars [28]. During the Summer Olympic Games in Central Park in Atlanta in 1996, a pipe bomb enclosed in a backpack exploded. Two people were killed and 112 were injured [29].

#### **Actors in the Model**

The panel has identified a list of actors whose behavior would be modeled for the different terrorist incidents. Each actor may represent a particular system or a set of systems, depending on its complexity. The actors used in any given simulation would depend on the particular scenario. Table 1 lists the actors and identifies their corresponding scenarios. A more detailed discussion of these actors is presented in the section entitled “Model Development Requirements.”

**Table 1. Actors and Scenarios**

<b>ACTOR</b>	<b>Scenario 1 Information Warfare</b>	<b>Scenario 2 Electric System Failure</b>	<b>Scenario 3 Biological Warfare</b>	<b>Scenario 4 Nuclear Warfare</b>
Federal Emergency Management Agency			X	X
Federal Reserve				X
Banking and Financial Investment Systems	X	X	X	X
Households	X	X	X	X
Medical Systems			X	X
National Guard		X	X	X
Industries/Firms	X	X	X	X
Federal Government	X	X	X	X
Telecommunications Systems	X	X	X	X
Transportation Systems	X	X	X	X
Electric Power Systems	X	X	X	X
State and Local Organizations	X	X	X	X
Life Support Systems	X	X	X	X

## **Simulation Output**

The proposed computer model would be capable of calculating three types of output at two different time frames, as discussed in the following subsections.

### **Output Types**

The three types of output are social impacts, economic costs, and organizational effectiveness.

- *Social impacts* refer to the effects of the terrorist incident on the affected population. Statistics would be computed, for example, on the number of deaths, illnesses, hospitalizations, homeless, and disabilities. Social response data would also be of concern (e.g., people leaving cities and blocking transport; looting; vandalism), as these actions would create additional burdens on government and military resources. In addition, the loss of critical resources such as food and water would be enumerated.
- Any of the terrorist acts could result in significant *economic costs* to the country. Primary data that would be calculated include the effects on regional economic activities, on the Gross Domestic Product (GDP), on employment,

on stocks and bonds, and on the loss of critical resources such as capital, buildings, and manufacturing.

- A key factor in mitigating the effects of any incident is the degree to which organizations have planned a coordinated strategy for immediate response and subsequent recovery. The *organizational effectiveness* of agencies responsible for responding to the myriad needs of victims in the affected area would be assessed by a set of criteria yet to be determined. The organizations (or actors) selected would be relevant to the particular scenario.

The panel envisions that a primary use of the model would be to determine the optimum degree of organizational effectiveness that is required to reduce the social impacts and the economic costs of any incident. In this manner, the computer model would be a useful planning tool both in preparing for possible incidents and in mitigating their effects should the incidents occur. The implementation features of the computer model would allow for user specification of scenario input parameters, supporting such optimization analyses as well as risk assessment. For example, the number of units available for the National Guard could be modified in subsequent model runs of the same terrorist incident to determine the maximum effectiveness of that actor based on the finite resources available.

### **Output Time Frames**

The computer model would be designed to calculate the three types of output at two different time frames: (1) the first 24 hours and (2) the first 30 days. The panel recognizes that the full economic impact of any incident would not be known for some time—possibly up to five years. Detailed modeling of the impact after 30 days could be addressed in a follow-on task to this project.

The behavior of different actors would be simulated based on the time frame selected. For the 24-hour frame, the emphasis would be upon the in-place, immediate response and the analysis would focus on the ability of the responsible agencies to interact and minimize the social impacts (e.g., loss of life). In general, the 30-day analysis would be concerned with the ability of the agencies to coordinate the recovery effort and thus minimize the long-term economic costs. However, for scenarios 3 and 4, minimizing the social impacts would also be critical.

### **Agent-Based Approach**

We assume that a computational model similar to Aspen will be built to simulate the terrorist events. Developed by Sandia, Aspen is an agent-based Monte Carlo simulation that runs on Sandia's massively parallel Intel Teraflop computer. Individual agents (actors) represent real-life economic decision makers, and aggregates of the agents' microeconomic actions generate macroeconomic variables [30].

The individual system models (those constructed for each of the actors in the proposed computer model) would likely constitute a reusable library of agents. Written in an object-oriented language, these agents could be dragged and dropped into different scenarios. With little or no modification, the agents could be applied to other terrorist acts that are subsets of the scenarios identified in this paper.

## **Model Development Requirements**

To build a computer model like that described herein requires an initial in-depth research and writing project, which is the level of effort (LOE) proposed in this paper. Information must be gathered about all of the actors identified so that we understand how they behave normally and also how they are likely to behave under stress. What, for example, are the responsible agencies' rules for responding to certain incidents? We must learn how these actors interact internally and with each other under normal and under extreme circumstances. We must develop a set of operations that the actors perform and then define the applicable operations in a logical sequence. We must be able to identify and quantify the resources on-hand and remotely accessible to the actors.

The result of this research and writing project would be a Requirements Specification Document. This document would provide a detailed description of how the computer model would be implemented, including finalized details about the scenarios, the actors, and the simulation output. The document would also contain a complete description of the operational behavior and attributes of each actor, including the actor's linkages with other actors. For actors representing complex systems, the description would be carried to the level of detail required for representing that complexity.

## **Modeling Needs for Actors**

The following subsections provide further information about the 13 actors and highlight important data that would need to be acquired and written models that would need to be developed in this proposed project to accurately represent the actors' participation in the terrorist incidents.

### **Federal Emergency Management Agency (FEMA)**

FEMA, an independent agency of the U.S. government, has leadership responsibilities for the nation's emergency management system. When the President has declared a major disaster, FEMA is responsible for coordinating its own response activities and the activities of up to 28 other Federal agencies. In these efforts the federal agencies assist states and localities in recovery by providing services, resources, and personnel to perform life supportive functions (e.g., transporting food and potable water, assisting with medical aid, and providing electric generators to keep essential facilities operational)

[31]. Per Presidential Directive 39, FEMA has the lead Federal responsibility to assist state and local governments in dealing with the consequences of a terrorist event [32].

For this project, FEMA's organizational structure, strategies, interagency alliances, and history would be studied. Models would be developed, for example, that describe the movement of materials and supplies, the availability of personnel, and the effectiveness of the agency's actions.

### **Federal Reserve**

Policies, interactions, and practices of the Federal Reserve to regulate the nation's financial systems are of interest. For this project, we would develop normal operational models, as well as models characterizing the emergency decision-making processes implemented by the Federal Reserve following catastrophic events. Under what conditions, for example, are decisions made to close banks? Further, what emergency systems (such as rediscounting) are available to member banks for acquiring additional funds. The availability of funds in affected areas could have considerable impact on reconstruction and rehabilitation efforts, which would be affected by the activities of regional Federal Reserve offices.

### **Banking and Financial Investment Systems**

Catastrophic events can impact many aspects of the country's financial systems. Our project would examine the economic impact of the terrorist acts on the banking system and on financial investment systems, most specifically the stock and bond markets. Modeling of electronic banking activities would be included in this effort. A significant business risk is the loss of faith by depositors in the security of their banks and by investors in the security of their portfolios [33]. Therefore, it is important to examine the controls established by banks and stock exchanges to reduce excessive volatility. According to Jinnett [33], the potential run on a bank would most likely be caused by large institutional investors because the Federal Deposit Insurance Corporation (FDIC) insures deposits up to \$100,000.

For banking, catastrophic events can also affect borrowers' ability to repay their current debt obligations and place many individuals and businesses in the position of seeking new loans to recover their financial strength. Accordingly, the project would focus on developing models describing the availability of disaster loans and alternatives for adjusting the terms of existing loans (e.g., credit cards and home mortgages).

### **Households**

This complex actor would encompass the actions, interactions, and choices of people in the immediate area of the terrorist incident. For this project, normal behavior models would need to be developed. Such models would describe routine activities such as going to work, buying homes, making investments, and seeking employment. Other models for

crisis-related behaviors would also be required. For example, what actions are people likely to take during times of confusion and panic? Will they get on the highways immediately and leave the area temporarily? Will they move permanently? Will they choose to help their family or their community first? Consequently, models describing the movement patterns of people must be developed, as these patterns may impact other systems' provision of rescue and relief services in the short term and the very viability of the city or region in the longer term.

### **Medical Systems**

The panel is interested in the medical community's capabilities to respond on-the-scene to terrorist incidents and to provide immediate and follow-up care within established medical centers. Models for medical first responders would be developed, including the triage system for delegating and prioritizing the care of victims. Because some victims would need to be evacuated from the scene or from the area, such models would incorporate linkages to the available transportation systems. Models for the provision of treatment at area hospitals and emergency care centers would incorporate the procedures and the on-hand and remotely accessible resources for responding to the incident type, including supplies, hospital beds, and personnel. The panel recognizes that the level of training of all medical personnel will be a critical factor in dealing with several of the terrorist incidents. Thus the medical models would consider the training factor.

### **National Guard**

The National Guard is composed of Army and Air Force units that serve with active duty Army and Air Force units at installations in the United States and overseas. There are currently 367,000 people in the Army National Guard and 109,000 people in the Air National Guard. In addition to serving as part of the nation's military force, the National Guard serves the states for emergency response and community support missions [34].

For this project, the provision of protective forces and services to the affected areas would be of interest. This support could include recovery of bodies, distribution of supplies and life support resources (food and water), setting up temporary shelters, guarding businesses, and other policing services required to restore civil order. As with other emergency personnel, the level of training received to manage certain types of terrorist incidents (i.e., biological and nuclear) would be factored into the incident-specific models.

### **Industries/Firms**

The proposed computer model would calculate the financial impact of the terrorist incidents on firms in the economy. For this project, models representing aggregates of the major types of industries would be developed, including those that produce durable goods (e.g., automobiles, appliances), nondurable goods (e.g., food, clothing), and those that provide services (e.g., education, insurance). Models would reflect regional economic

conditions as well as national aggregates to facilitate linking the four terrorist scenarios from region-specific to national financial impacts. It is possible that certain types of industries could be victims in some of the terrorist scenarios and suppliers in other of the scenarios.

### **Federal Government**

This complex actor, a system of systems, would require a number of written models to describe the structures, roles, and operational behaviors of the President, Congress and other federal agencies involved in responding to terrorist acts and managing the consequences of these acts. Note that FEMA would be treated as a separate but intricately linked actor.

In its 1997 report, the General Accounting Office (GAO) [35] noted that more than 40 federal agencies, bureaus, and offices were involved in combating terrorism. While not all of these organizations would play a major role in the strategies captured by the proposed computer model, the issues of coordination and communications among the selected agencies and other actors (like state and local organizations) would need to be examined and characterized. The effects of multiple decision-makers, some with potentially overlapping or higher-priority responsibilities, could result in delays that impede the success of response and recovery efforts. The panel specifically cited investigative delays as a potential problem.

Key U.S. government agencies that would be included as part of the Federal Government actor include the Department of Defense (DoD), FBI, Public Health Service (PHS), Environmental Protection Agency (EPA), Department of Energy (DOE), Department of Justice (DoJ), Department of Transportation (DoT), U.S. Department of Agriculture (USDA), General Services Administration (GSA), and National Communications System (NCS). These agencies are members of the Senior Interagency Coordination Group on Terrorism, which is co-chaired by FEMA [36].

### **Telecommunications Systems**

Modeling of the telecommunications industry must demonstrate the dependence and reliance of our society on the timely transmission and receipt of information. It must also show fidelity to the intricate and complex interdependence of all society's institutions, as current efforts to address the Year 2000 problem are making ever more clear. In recent testimony before the U.S. Senate, FCC Chairman William Kennard stated:

The communications infrastructure is absolutely critical, not only to the economy, including the general commerce, transportation and banking sectors .... but also to national preparedness, military, public safety, emergency and personal communications.

Every sector of the communications industry -- broadcast, cable, radio, satellite, and wireline and wireless telephony -- could be affected: the United States Emergency Alert System relies on television and radio broadcasts, the transmission of which may be affected by the Year 2000 problem; in some areas of the country, radio, cable and satellite systems are the only sources of up-to-date news and information; and police, fire departments and other emergency personnel rely on radio systems to communicate. We must ensure that all of these forms of communications continue uninterrupted [37].

For this project, models would be developed to describe the normal and crisis-mode operational behaviors, resources, and capabilities (e.g., networks) of representative telecommunications service providers in private industry, including Internet providers. Of particular interest is the degree of intra-industry cooperation in the event of a national emergency. Models would also be developed for special government capabilities of the National Communications System (NCS), like the Government Emergency Telecommunications System (GETS).

### **Transportation Systems**

The ability to move equipment, supplies, and support personnel into, through, and out of a disaster-stricken area is critical. The computer model, therefore, must be capable of treating the major forms of transportation that can service the area, including trucking, air, rail, bus, local delivery services, shipping, and even personal vehicles. For the commercial and public systems, it would be important to determine their general operating procedures, availability of personnel and vehicles/equipment, and contingency planning for emergencies. Just-in-Time delivery systems may be highly vulnerable in several of the threat scenarios. Under a general umbrella of such vulnerabilities, would normally competitive industries cooperate to assist in the relief and reconstruction efforts?

As part of developing models for the transportation systems, we would also be interested in determining the supply, storage, and distribution of fuel systems (oil and gas) under normal and abnormal periods in the affected areas. It is understood that these fuel systems are critical to other aspects of the economy besides transportation, and their usage by residential, commercial, industrial, and electric utility users would be treated as separate from that used in transportation.

### **Electric Power Systems**

Scenario 2 deals directly with disruption of electric power in a major region of the United States. Other scenarios, however, through a series of interconnected events, could also result in power outages. In these scenarios, as in our routine lives, our dependence on electricity and the electric power systems' interdependence with itself and other systems can be poignantly demonstrated. Without electricity, there are no lights, no computers, no

refrigeration, no air conditioning, no factory production. It is a dark world and for many it also could be very cold, as few methods of heating work without electricity.

An electric power system disruption of the magnitude perceived for Scenario 2 could result in loss of synchronism within the region's high-voltage transmission network. Loss in such control can result in widespread outages such as affected the Western transmission network on July 2 and August 10, 1996 [38]. (The Western network is one of four major synchronous interconnections that compose the North American power grid [39]). Local events like line sags resulting from hot weather and misoperation of relays created electrical disturbances that spread throughout the network. Power to millions of customers in several states and in areas of Canada and Mexico was disrupted. Financial losses suffered by California industry for the August 10 incident were estimated in the range of \$1-\$3 billion [38].

For this project, models would be developed of electric system providers' procedures for normal and extreme contingencies, available equipment and personnel for such contingencies, and reserves to accommodate system failures. The models of electric system failures and outages would include the restoration process. If transmission lines were destroyed, then the model would include those actions necessary to accurately represent the time scale.

### **State and Local Organizations**

Formal state and local organizations, both governmental and nongovernmental, that play a role in providing support to communities and families during normal and crisis events would be studied. Models would be developed describing the roles and coordination characteristics of emergency first responders (including police, firefighters, and rescue services), state and local government agencies, and charitable organizations (e.g., churches, Red Cross, Salvation Army). Note that the emergency services provided by medical personnel and by the National Guard would be treated as separate actors in this project. Appropriate linkages among all systems that comprise the State and Local Organizations actor would be developed, as would linkages from this actor with all other relevant actors for the particular scenarios.

### **Life-Support Systems**

Modeling of this actor would focus on the capabilities of the local/regional water supply and food distribution systems to deal under normal and adverse circumstances. As noted by the President's Commission for Critical Infrastructure Protection [9], a safe and on-demand water supply that is delivered at significant pressure is crucial for users. Consequently, procedures for dealing with the contamination and/or disruption of the water supply would be addressed, as well as the potential safety and economic consequences. For the scenario that treats biological contamination of the water supply system, the spread of disease would be of particular concern.

As with water, the safety and availability of food products is critical following disasters. The cascading effects of terrorist acts or natural disasters on telecommunications, transportation, and electric power systems can trigger a breakdown in the food distribution network. Supermarkets can run out of food, and food requiring refrigeration will spoil. On-hand supplies and operational procedures during normal and crisis events would be documented for the supermarket chains and their distributors. Other sources of safe food supplies and methods for obtaining them inside and outside the area would also be identified and modeled.

## Proposed Level of Effort (LOE)

Based on limited discussion and our experience, the panel estimates that the LOE for this project will require 234 man-months (mm) to develop a complete description of the model. Table 2 summarizes the key modeling needs and lists the time required to develop individual models for each of the actors. The table also includes the time for preparing the final Requirements Specification Document into which the individual models would be embedded.

**Table 2. Model Documentation Requirements**

<b>Actor</b>	<b>Summary of Key Modeling Needs</b>	<b>LOE (mm)</b>
Federal Emergency Management Agency	policies and procedures, command structure, movement of materials and supplies, personnel availability, effectiveness of actions	24
Federal Reserve	normal models, decision process to close banks	2
Banking and Financial Investment Systems	normal banking models, disaster loans, alternatives to repayment, stock and bond markets	16
Households	normal behavior models (e.g., seeking employment, buying, making investments), confusion and panic, movement and decision-making in crisis	24
Medical Systems	models of medical first responders; normal and crisis-behavior models for hospitals, emergency care centers, and other special medical facilities; medical supplies	24
National Guard	provision of protective forces, services, and supplies	12
Industries/Firms	normal economic models for producers of durable goods, nondurable goods, and services	12
Federal Government	Presidential and Congressional Acts and Orders, reaction mode, investigative delays, other Federal agencies	24
Telecommunications Systems	normal and crisis-behavior models for representative service providers (telephone, cable, wireless, satellite, broadcast, radio, Internet)	12
Transportation Systems	models describing the movement of materials via trucking, air, rail, shipping, and delivery services	12

**Table 2. Model Documentation Requirements**

<b>Actor</b>	<b>Summary of Key Modeling Needs</b>	<b>LOE (mm)</b>
Electric Power Systems	normal and extreme contingency models, reserves, personnel, electric grid networks, power suppliers	24
State and Local Organizations	models of police, firefighters, rescue services, state and local governments, and charitable organizations	24
Life Support Systems	food, water, effects of contamination	12
Requirements Specification Document	finalize details about all model components; incorporate individual models into document	12
<b>Total</b>		<b>234</b>

## **Summary and Future Directions**

The computer model proposed in this paper would be able to support the analysis of complex interactions and decision-making processes among various systems in our country in environments that would likely tax the capabilities of these systems and require high levels of cooperation. Representation of these intrasystemic and intersystemic relationships requires a detailed and comprehensive LOE to capture the characteristics and operational behavior of these systems under normal and stressed circumstances. The real-life incidents cited in this document and others encountered during the information-gathering process would provide a historical record of the behavior of certain systems under stress.

Development of the initial model requirements was accomplished in a brief three-hour session by a panel of scientists with expertise in designing, developing, implementing, and evaluating complex model-based simulations. To accomplish the LOE defined herein, Sandia brings its collective and proven expertise in computational and information sciences, engineering sciences and system analysis, and surety science (which focuses on the safety, security, and reliability of energy and other critical infrastructures). As a national security laboratory for DOE, Sandia performs a wide variety of energy research and development projects and works on assignments that respond to military and economic threats to national security.

The LOE defined in this paper does not include an estimate for actual software coding of the computer model. We estimate that the actual coding effort would take from one-half to three-fourths of the time required to complete the written description. Until details of the model components are gathered, it is not reasonable to project the actual coding estimate.

As noted previously, the proposed computer model would be designed to calculate the economic costs of the terrorist incidents for up to thirty days. Expansion of this capability to one or even five years could be accomplished with an extension to the model

to more realistically assess the economic costs to geographic regions and the country of the terrorist incidents. In such an extension, the effects on the global economy could also be considered.

## References

1. M. Liu and M. Mabry, "Massive Manhunt," *Newsweek*, August 24, 1998, 30-32.
2. J. C. McKinley, Jr., "Bombing Toll Rises as Rescue Effort in Nairobi Intensifies," *The New York Times*, August 9, 1998, Available: <http://www.nytimes.com>
3. T. Weiner, "1800 Injured Overwhelming Kenya Hospital," *The New York Times*, August 9, 1998, Available: <http://www.nytimes.com>
4. E. M. Lederer, "Death Toll Rises in Africa Blasts," *The Associated Press*, August 8, 1998 2145EDT, Available:  
<http://www.aol.com/mynews/news/story.adp/cat=0100&id=1998080>
5. "Witnesses Endorse Nunn-Lugar-Dominici Program," April 22, 1998, Available:  
<http://web.iquest.net/lugar/rgl042398.htm>
6. U. S. Department of Defense, *Department of Defense Report to Congress Volume I, Domestic Preparedness Program in the Defense Against Weapons of Mass Destruction*, May 1, 1997, Available:  
<http://www.fas.org/spp/starwars/program/domestic>
7. Federal Bureau of Investigation, "FBI in Partnership," Available: <http://www.fbi.gov>
8. D. Watson, "Foreign Terrorists in America: Five Years after the World Trade Center," Statement before the Senate Judiciary Committee Subcommittee on Technology, Terrorism, and Government Information, United States Senate, February 24, 1998, Available: <http://www.fbi.gov/congress/wtc.htm>
9. President's Commission on Critical Infrastructure Protection, *Critical Foundations*, October 1997, Available: [http://www.pccip.gov/report\\_index.html](http://www.pccip.gov/report_index.html)
10. Statement of Dr. Jeffrey A. Hunker, Director of the Critical Infrastructure Assurance Office before the House National Security Committee, Military Procurement Subcommittee, Military Research and Development Subcommittee, June 11, 1998, Available: <http://www.ciao.gov/sbhunker11june1998.html>
11. Federal Bureau of Investigation, "Mission," Available:  
<http://www.fbi.gov/nipc/mission.htm>

12. Critical Infrastructure Assurance Office, "Richard A. Clarke, A Biographical Sketch," Available: <http://www.ciao.gov/bioclarke.html>
13. "Jeepers Creepers: One Malfunction Knocks Out 40 Million US Beepers," *The Washington Post*, May 22, 1998, Available: <http://www.smh.com.au/news/9805/22/text/world20.htm>
14. The Center for Strategic and International Studies, "The Y2K Crisis: A Global Ticking Time Bomb?," Y2K Conference, June 2, 1998, Available: <http://www.csis.org.html/y2ktran.html>
15. B. Pietrucha, "Paging Services Back Online Across Most of US," *Newsbytes News Network*, May 22, 1998, Available: <http://www.newsbytes.com>
16. The Associated Press, "PamAmSat Says Service is Restored to Pagers," *Florida Today Space Online*, May 22, 1998, Available: <http://www.flatoday.com/space/explore/stories/1998/052298s.htm>
17. D. Dietz, "PAGE ONE -- PG&E Workers Questioned by FBI on S. F. Blackout," *San Francisco Chronicle*, October 25, 1997, Available: <http://www.sfgate.com/cgi-bin/article.cgi?file=/chronicle/archive/1997/10/25/MN35969.DTL>
18. D. Dietz, "PAGE ONE -- FBI Probes S. F. Blackout," *San Francisco Chronicle*, October 24, 1997, Available: <http://www.sfgate.com/cgi-bin/article.cgi?file=/chronicle/archive/1997/10/24/MN1658.DTL>
19. *The Report of the Ministerial Inquiry into the Auckland Power Supply Failure*, July 1998, Available: <http://www.moc.govt.nz/inquiry>
20. M. Boland, "Inner-city People Rejoice in Placing of Blame," *New Zealand Herald*, July 22, 1998, Available: <http://www.herald.co.nz/nzherald>
21. "Auckland CBD Hit by Blackout Again," *The Straits Times Interactive*, May 11, 1998, Available: <http://web3asia.com.sg/archive/st/3/pages/stwrld22.html>
22. A. Anderson, "Radio and TV Stations Affected by Power Crisis in New Zealand," *Online New Zealand News*, March 5, 1998, Available: <http://www.ened.com/akltv.html>
23. "Auckland Celebrates Power to the People," *BBC News Online: World: Asia-Pacific*, March 27, 1998 10:45 GMT, Available: <http://news.bbc.co.uk/hi/english/world/asia%2Dpacific/newsid%5F70000/74057.stm>
24. M. Yamajuchi, "On Anniversary of Subway Nerve-Gas Attack, Japan Mourns Victims," *Source News and Reports*, March 20, 1996, Available: [http://www.sddt.com/files/library/wire/96wireheadlines/03\\_96/DN96\\_03\\_20.html](http://www.sddt.com/files/library/wire/96wireheadlines/03_96/DN96_03_20.html)

25. R. Danzig, "Biological Warfare: A Nation at Risk – A Time to Act," *National Defense University Strategic Forum*, Number 58, January 1996, Available: <http://www.ndu.edu/ndu/inss/strforum/forum58.html>
26. J. M. Deutch, "DCI Speech," *Conference on Nuclear, Biological, Chemical Weapons Proliferation and Terrorism*, March 23, 1996, Available: [http://www.cia.gov/cia/public\\_affairs/speeches/archives/1996/dci\\_speech\\_052396.html](http://www.cia.gov/cia/public_affairs/speeches/archives/1996/dci_speech_052396.html)
27. Federal Bureau of Investigation, "World Trade Center Bombing," Available: <http://www.fbi.gov>
28. Federal Bureau of Investigation, *Terrorism in the United States*, Available: <http://www.fbi.gov/publish/terror/terroris.htm>
29. Federal Bureau of Investigation, *Terrorism in the United States 1996*, Available: <http://www.fbi.gov/publish/terror/terrusa.htm>
30. N. Basu and R.J. Pryor, *Growing a Market Economy*, Sandia Report, Sandia National Laboratories, Albuquerque, NM, October 1996.
31. Federal Emergency Management Agency, *Strategic Plan FY 1998–FY 2007*, Available: [http://www.fema.gov/library/spln\\_1.htm](http://www.fema.gov/library/spln_1.htm)
32. Testimony of Steven G. Sharro, Acting Director of FEMA's Terrorism Coordination Unit, before the Military Research and Development Subcommittee House Committee of National Security, Hearing on "Federal Response to Domestic Terrorism Involving Weapons of Mass Destruction - Training for First Responders," Indianapolis, Indiana, March 21, 1998, Available: [http://www.fas.org/spp/starwars/congress/1998\\_h/3-21-98sharro.htm](http://www.fas.org/spp/starwars/congress/1998_h/3-21-98sharro.htm)
33. Testimony of Jeff Jinnett, President of LeBoeuf Computing Technologies, L.L.C., before the U. S. Senate Banking, Housing and Urban Affairs Committee, Subcommittee on Financial Services and Technology, July 10, 1997, Available: <http://www.fas.org/2000/y2K/congress/jinnett.htm>
34. "The National Guard in a Nutshell," Available: <http://www.ngb.dtic.mil/>
35. R. Davis, *Combating Terrorism: Observations on Crosscutting Issues*, GAO/T-NSIAD-98-164, Testimony before the Subcommittee on National Security, International Affairs and Criminal Justice, Committee on Government Reform and Oversight, House of Representatives, April 23, 1998, Available: <http://www.fas.org/irp/gao/nsiad98164.htm>

36. DoD Tiger Team, *Department of Defense Plan for Integrating National Guard and Reserve Component Support for Response to Attacks Using Weapons of Mass Destruction*, January 1998, Available:  
<http://www.fas.org/spp/starwars/program/wmdresponse/rpt/index.html>
37. Statement of William E. Kennard, Chairman of the Federal Communications Commission, before the Committee on Commerce, Science and Transportation, United States Senate on Year 2000, April 28, 1998, Available:  
<http://www.fcc.gov/speeches/Kennard/Statements/stwek824.html>
38. Electric System Reliability Task Force Secretary of Energy Advisory Board, *Technical Issues in Transmission System Reliability* (A Position Paper), May 12, 1998, Available: <http://www.hr.doe.gov/seab/techissues.pdf>
39. U. S. Congress, Office of Technology Assessment, *Physical Vulnerability of Electric System to Natural Disasters and Sabotage*, OTA-E-453, Washington, DC: U. S. Government Printing Office, June 1990.

## Distribution

1	MS	0151	G. Yonas, 9000
1		0321	W. J. Camp, 9200
1		1165	J. Polito, 9300
1		0741	S. G. Varnado, 6200
1		9004	M. John, 8100
1		1165	D.M. Rondeau, 9301
50		1109	R. J. Pryor, 9202
10		1207	M.S. Allen, 5909
10		0749	O.H. Paananen, 6217
10		1217	K.L. Hiebert-Dodd, 5913
1		0129	N. Singer, 12620
1		9018	Central Technical Files, 8940-2
2		0899	Technical Library, 4916
1		0619	Review and Approval Desk, 15102, For DOE/OSTI