

# **Safeguarding the Homeland: Governors & Mayors Speak Out**

## **Chapter 1: The Role of the Private Sector in Homeland Security**

Professors Simon Hakim and Erwin A. Blackstone

### **1. Introduction**

In 2002 the total homeland security budget was \$20.6 billion with a supplemental as a result of 9/11 of \$12.36 billion. The proposed federal budget for 2008 is \$61.16 billion, an almost 100 percent increase in 5 years. In 2008, one third is spent on border and transportation security, almost another one third on protecting critical infrastructures and key assets, and about eight percent on emergency preparedness and response. (OMB, 2008)

In spite of the substantial increase in federal spending, only one quarter of state emergency operations plans and 10 percent of municipal plans are sufficient to cope with a natural disaster or terrorist attack (Flynn, 2007:5). The majority of plans “cannot be categorized as fully adequate, feasible or acceptable to manage catastrophic events” (U.S. Department of Homeland Security June 2006). In addition, a well-regarded non-governmental commission argued that additional funding of \$98.4 billion over five years was required to cover potential emergency response needs. This figure does not include overtime, training, and police force needs across the U.S. (Council of Foreign Relations, Rudman Report, 2003: 31). There is an obvious lack of financial resources, and all expect the federal government to carry the burden.

The financial burden is huge since the amount of critical infrastructures includes 15,000 chemical facilities, 489,862 miles of pipelines for hazardous liquids and natural gas, 5,389 public use airports, 16,024 publicly-owned wastewater treatment facilities, 700,000 miles of drinking water system, and 64 nuclear power reactors (Critical Infrastructures, 2008).

After 9/11, billions of tax dollars have been spent creating a new capability to deal with crises in the U.S. The U.S. Department to Homeland Security was established and increased funding was made available to emergency responders. Exercises to prepare for mass casualty events were

held across the U.S. Nevertheless, hurricanes Katrina and Rita proved that we were no more capable of responding to a major catastrophe than we were on 9/11 (Clark et al, 2006:1).

The attack of 9/11 and the natural disasters of Rita and Katrina showed that the US lacked appropriate communications, supplies, and possibly suffered from inappropriate management during emergency events.

The objective of this chapter is to provide guidance for:

1. Improving the public sector's structure and responsibilities to better meet demands in major homeland security events.
2. Engaging the private sector in fulfilling homeland security obligations, providing incentives and challenges, and appropriate regulations.
3. Establishing regulated insurance programs to achieve business survival following a major uncertain homeland security event. The insurance program will also motivate businesses and individuals to take appropriate precautions to minimize adverse effects.
4. Introducing technological products that could supplement or substitute for regular labor efforts. Since 9/11 many IT companies have been developing products to avoid the problems faced in New York City during and following the attack. The chapter will review the problems associated with response and recovery from homeland security incidents and present technological solutions employed by state and local governments.

## **2. Background**

As a result of the 10<sup>th</sup> amendment to the U.S. Constitution, the states have all the powers not expressly delegated to the Federal Government. This has been interpreted as the “police power”

where the states have the ultimate control of most emergency services. In practice, the states allow local governments to be the principal responders and managers in case of disasters. When a terrorist or natural disaster occurs, the local jurisdiction responds while the State may aid with the state police, the National Guard, and other resources. However, the ultimate control is with the governor who may choose to exercise control under unusual circumstances. The Governor may declare a State of Emergency in order to mobilize and send in the National Guard.

The federal government basically provides assistance to states and localities when an emergency occurs beyond the capability of the state. The Federal Emergency Management Agency (FEMA) often supplies medical equipment, temporary housing, food, and other essentials. The President may make a Disaster Declaration in order to provide greater federal assistance. This includes loans or grants to homeowners, businesses, and local governments to recover from disasters.

The management of disasters is done by the mayor under the authority of the state and is usually handled by the chiefs of the police and fire departments. The mayor can clearly choose personally to manage the response and recovery efforts.

Small natural and manmade disasters occur often and thus sufficient response and recovery experience exists. There are, after all, the lessons learned from the multitude of small terrorist attacks in Israel and from “regular” natural events here in the US. However, such catastrophes as 9/11 and Hurricanes Katrina or Ike show that the usual practices and material support are insufficient for major disasters. Government at all three levels has responded by developing either new departments for homeland security or created positions to deal specifically with homeland security.

Homeland security (HLS) is viewed as a pure public good. If adequate HLS services are provided then most residents will enjoy the benefits. Further, private marginal costs of homeland security are higher than private marginal benefits, and the latter are significantly lower than social marginal benefits. Thus, there is little incentive for individuals to expend resources on HLS services. Given these facts, it is not surprising that HLS services are considered by all a primary responsibility of government at all three levels. The federal government is expected to

cover the cost since it has the greatest ability to pay and the negative externalities associated with disasters are normally far more widespread than within any individual state.

Market failure exists also in the private sector and especially with respect to corporate resource allocation. Long run profit maximization may suggest greater corporate spending on security. However, the interest of top corporate executives is to earn short-term profits even at the expense of the long-term. Executives' personal interest is high immediate profit since that is what determines their compensation and tenure on the job. Also, short-term profits keep the stock price high and prevent hostile takeovers. Executives do not maintain their positions for too long, and thus the consequences of lack allocation for security will inure to others. Supporting the notion of the short term horizon of corporate executives is the fact that since 2002 Sarbanes-Oxley Act, corporate turnover has increased. Specifically, there was a 91.3 percent increase in the departures of the top 100 Fortune CEOs compared with the previous five year period. The global business environment adds to the competitive pressures for short term profits and to reduced incentives for security spending. Almost twenty percent of Fortune 500 companies do not even have a corporate security officer to manage threats and security risks. (Blades, 2008).

The next question is how to allocate limited resources among the three categories in homeland security: preparation-prevention, response, and recovery in a manner that maximizes security. It is commonly believed that most resources be spent on target hardening which is the form of prevention. Others argue that static or inflexible measures are inefficient. The number of critical infrastructures is huge; the terrorist has complete choice of target, timing and attack method. Effective prevention measures are very costly and ineffective; a well prepared team of terrorists could easily overcome a static, unprepared group of guards. Instead, efforts should be placed on effective response and recovery. For example, it is possible to place a guard at the entrance of each school and build a high fence to prevent an attack on students. Clearly, such measures could not deter or prevent a team of terrorists who plan an attack on a specific school. Instead, digital data could be maintained on the buildings, hidden cameras installed at the school, and a well trained and mobile SWAT team could be available for each metropolitan area to deal with any attack on critical infrastructures.

The government could encourage deployment of technology to improve homeland security. Technological innovations that could improve homeland security relate to a computerized automatic protocol response system, managing the event over the Internet, sufficient and durable communication channels among the key people during the event, data mining to anticipate and perhaps prevent an event, reverse 911-emergency notification systems, and use of digital monitoring devices.

Technological products could serve both as a substitute for or a complement to labor. Unlike the private market, signals of need or incentives of profit are less present in the public sector. Even though officials at the IT departments of government may know their needs, there are no markets to encourage appropriate or prevent excessive adoption of new technology products. Unlike the private sector, financial incentives are weaker for government decision makers, the bureaucracy is greater, and therefore adoption of new products is less likely to occur. The more rapid diffusion of e-commerce versus that of e-government supports our argument (Blackstone et al, 2005: 4).

Managerial innovations include establishing a separate command and response structure once an emergency event occurs, creating emergency forces for such an event, creating emergency positions and responsibilities for public employees, and sharing relevant security information among public and private agencies.

### **3. Restructuring Public Emergency Services**

State and local governments provide emergency response services, some of which lack public goods attributes. In this section we shall identify services that should not be provided by public police, fire, and ambulance entities, estimate their magnitudes, and analyze whether social welfare will be affected by their elimination from the public sector. Other emergency services are public in nature but could be contracted out and provided under competitive conditions. In both cases, government could provide such services within a competitive market context. We shall then outline how the saved resources could be shifted and used for homeland security purposes.

Police services that do not involve public good attributes include attending and investigating minor traffic accidents, escorting funerals and oversized vehicles, animal control, unlocking vehicles, recording citizen complaints, checking on people's welfare, and traffic control during road construction. The largest single item on police budgets is response to burglar alarms of which 94-99 percent are false. Elsewhere we showed that police response is a public good only when a real burglary occurs, and there is a chance of apprehending a burglar. When alarm owners accidentally activate their systems or when a system malfunctions, there are no social benefits when police respond. If police eliminate provision of the above non-public services, private entities will enter under competitive market conditions. Further, non-users of these services in the community will then not be required to subsidize those who use them, the service will be provided to its users by private entities, and social welfare will not diminish. Alternatively, police should charge their long run average total cost and allow competitors to also respond to alarms. Our calculations show that if police indeed eliminate the delivery of non-public goods, 13 percent or 55,000 patrol officers could effectively be used for other services with no social loss. In dollar terms the total annual savings will be \$2.8 billion (Blackstone, Buck, and Hakim, 2007).

Police are a public monopoly in providing most of their services. Some public services could be produced under market conditions where many potential suppliers exist. This will most likely improve efficiency in their provision. Police could contract out such public good services as handling abandoned vehicles, providing criminal information databases, enforcing traffic and parking regulations, providing lost and found services, guarding prisoners, protecting court rooms and public infrastructures, processing reports, and fulfilling office administrative duties. Government should employ Activity Based Accounting (ABC) where expenses are attributed to particular functions or activities that are considered for contracting out. Only then can government assure that the lowest bidder actually saves resources.

Basically, wherever civilian workers replace expensive sworn officers, savings on the order of 30 percent will be realized. Contracting out will lead to an additional annual savings of \$1.15 billion or the equivalent of 23,000 officers (Hakim, Buck, and Blackstone, 2007). In small

communities, the police may have to provide services since the market is too small to accommodate competitive entry. In any event, the police should charge for non-public services and competitive entry should always be allowed.

Extinguishing fires is a public good since fires spread and cause harm and injury to others. However, responding to a false alarm is not a public good. If a resident overheats his stove causing a false alarm and a fire engine responds, other community residents gain no benefits while bearing a long run marginal cost between \$365 and \$1,050. Fifty-eight percent of fire responses are to false calls. By charging for false activations, the number of false alarms will be significantly reduced and they will not burden public budgets. Also private companies or other response entities should be allowed to compete with the public fire department. We estimated that if false alarms are eliminated between 18,600 and 48,900 fire-fighters or equivalently between \$0.93 billion and \$2.44 billion could be saved or reallocated to other uses. By pricing false alarms and enabling competitors to enter, cost of production will diminish, service level would remain the same, and social welfare will rise.

Ambulance services are not a public good, since individuals are served with no external effects and service could be denied to those unwilling to pay. However, government involvement is justified on the basis of the high value of life. In any event, government provision is not necessary since private ambulance services do exist.

A major problem facing ambulance services is the 25 percent or \$8.5 million calls a year are false. Local governments bear most of the \$0.92 billion cost for the false service responses, or equivalently, they could shift 18,300 first responders to more productive uses. Indeed, some use ambulances to reach the hospital for minor illnesses. This adds an additional burden on hospitals and governments (Blackstone, Buck and Hakim, 2007).

Evidence exists that private providers are more efficient and may provide higher quality care than public ambulances. Thus, exposing government ambulance companies to competition or contracting out through competitive bidding is desirable. Successful managed competition

requires that the public provider price at long run marginal cost and entry by other public or private providers is allowed.

Under the assumption of perfect information, the solution of managed competition would be preferred to contracting out where temporary monopoly is awarded after competitive bidding. Ambulance service companies, however, must be able to provide timely, high quality service anywhere in the community. Users of emergency services are usually unaware of quality differences among providers. Thus, in this imperfect information environment, contracting out where government assures quality service at a certain price may well be the preferred solution over managed competition.

### **Annual Savings from Elimination and Contracting out of Services**

<b>First Responders</b>	<b>Annual Savings</b>	<b>Number of responders that could be reallocated</b>
<b>Police</b>		
Elimination of false alarm response	\$1.8 billion	35,000
Elimination of other non-public goods activities	\$1.0 billion	20,200
Contracting out services	\$1.15 billion	23,000
<b>Fire</b>		
Elimination of false alarm response	\$0.93-2.44 billion	18,600-48,900
<b>Ambulance</b>		
Elimination of false alarm response	\$0.92 billion	18,300
<b>Total</b>	<b>\$5.80-\$7.31 billion</b>	<b>115,100-145,400</b>

**Source:** An earlier version appeared in Blackstone, Buck, and Hakim, 2007: 319.

Some suggest that in times of emergency, all emergency resources will be devoted in any case to homeland security. Homeland security activities, however, are not restricted to the time of the occurrence. On-going homeland security efforts include training of first responders who will operate during such events, developing plans, procedures and protocols to manage emergency

situations, conducting desktop exercises, and acquiring equipment and facilities. Other activities include acquiring special supplies like medicines, canned food, rescue equipment; purchasing, installing and training with interoperable communication systems; developing and training with robotic technology to dismantle bombs; and building and equipping an emergency center. The resources expended on non-public goods or the resources saved by encouraging greater efficiency could be used to accomplish the above activities.

Previously we reported that the Council on Foreign Relations (The Rudman Report) concluded that there was a \$98.4 billion shortfall in homeland security spending over a five year period. Specifically, by eliminating non-public goods and exposing other public goods to competition through contracting out, between 30 and 37 percent of the required funding could be obtained entirely from within the emergency services sector.

#### **4. Engaging the Private Sector in Homeland Security**

Demand for emergency personnel and equipment is higher when an emergency occurs than in normal circumstances. This is similar to the case of electricity where the capacity of power stations must be sufficient to meet peak time demand. Since electricity cannot be stored, capacity and production need to accommodate fluctuating demands. In order to save on infrastructure investment, prices could be established such that peak demand is smoothed out; the success of course depends upon price elasticity of demand.

Instead of a summer peak for air conditioning, HLS involves a natural disaster or a terrorist incident. However, most personnel and equipment are designed for off-peak demand and there is no a-priori knowledge about the probability of an event's occurrence, the nature of the event, the extent of the damage expected, and the types and extent of necessary resources to cope with the event. Since a homeland security event involves unknowable information, most, if not all, communities are unprepared for a major event and indeed may have little incentive to be prepared for the peak time demand. Unlike electricity where considerable experience exists about capacity utilization, no such information is available for terrorist events.

A consequence of the above peak time unknowable information situation is that most communities do not expend sufficient resources for homeland security and instead expect the federal government to undertake the responsibility. However, the amount needed to provide for a nationwide preparedness for major events is huge and cannot easily be accommodated by the federal budget. The experience of Rita and Katrina in Louisiana five years after 9/11 proved that the US is still unprepared. Given this lack of appropriate incentives by the players, it is apparent that government at all three levels is still not prepared for another major event.

In view of the above, we suggest forming a Public Private Partnership that could fulfill any conceivable excess demand resulting from a major event when public resources are insufficient. The objective is to provide financial incentives that will encourage private participation in homeland security efforts. Emergency legal homeland security jurisdictions should be formed to incorporate an entire affected area. In case of a catastrophic event, the emergency jurisdiction will likely encompass an entire metropolitan area and will not necessarily correspond with political boundaries.

In terms of personnel, private security forces are three times as large as the sum of federal, state, and local law enforcement officers (Bureau of Justice Statistics, 2005). The majority of them are low paid hourly workers with limited or no fringe benefits. It is possible to form civilian reserve units that can be mobilized in case of a catastrophic event. Also, retired police officers, fire fighters, and ambulance paramedics, as-well-as emergency managers could serve in these units. Training including emergency exercises could be performed during the year and the assignment of emergency personnel could be arranged for emergency situations. These people would be paid for their reserve duties. These earnings would probably be an adequate inducement to participate in such reserve force. In case of a real event, these reserve officers report to their pre-assigned responsibilities to perform the services for which they were trained.

Mayor Menino of Boston in chapter 2 discusses the creation of reserve medical units that can be mobilized in case of an emergency. In case of a major event like a biological attack, the existing medical personnel may not suffice. Pre-arranged and trained medical units composed of various medical and administrative volunteers handle the peak time demand. Mayor Drake of

Beaverton, Oregon evaluates (chapter 3) the establishment of a regional emergency response organization, which included public, private, non-profits, and volunteer groups. Volunteer groups play an important role in emergency response and recovery plans and efforts. During a major flood in 1996, a church staffed a flood information and referral line. Volunteers in an organization termed the Minutemen already operate on the southern US border to locate and identify illegal aliens who can then be apprehended by the US border patrol. This group's presence presumably deters some illegal entry. However, their activities raise such liability issues as illegal arrests and improper use of weapons. James Carafano suggests in chapter 4 that volunteers could be integrated within a State's defense forces to function under the Governor's control. This could alleviate some of the control and liability problems posed by vigilantes. Mayor Peyton of Jacksonville, Florida indicates in chapter 5 that his City has also been training volunteers to supplement first responders during an emergency. Further, Jacksonville firefighters, sheriff deputies, and many civilian city employees have been trained in disaster response. In particular, some city employees have been trained as call takers to serve during disasters or other peak time situations. Kirschenbaum shows in chapter 6 how Israel overcomes suicide bombing and other terrorist attacks against civilians; volunteers play an important role when an attack occurs. Included are civilian watch, reserve medical officers, and religious organizations that gather body parts. Since so many Israelis have military experience, even unorganized volunteers assist in emergencies.

An issue in integrating private security guards and retired emergency services' officers in homeland security efforts is whether such integration is likely to succeed. Indeed, there are many examples of successful cooperation between police officers and private guards. In New York City more than 1,000 private security organizations are linked with the police to prevent, prepare for, and respond to homeland security incidents. They work together on building evacuation plans, security screening of vehicles entering facilities and adjacent parking, checking suspicious individuals and packages, and sharing terrorism alerts (BJA, 2005: 11). In Las Vegas, private security forces guide police in casino related criminal events, and the police train private security in proper procedures for handling the usual criminal incidents (BJA, 2005: 15).

An interesting issue is obtaining recruits for the top and mid level reserve emergency management positions. Current practice in the US is that the local political leader is in charge of all emergency services in both regular and emergency situations. However, since the areas impacted during a catastrophic event are often larger than political jurisdictions, there could be a management cadre different from existing political structures. Successful local business and corporate leaders may be challenged by the opportunity to manage significantly large public security obligations. Already, local private executives occupy top local public positions like weak mayors in such major cities as Phoenix, AZ and Charlotte, NC or chair county executive boards like Orange County, CA. The incentives for top and middle level homeland security management personnel clearly differ from the financial incentives already suggested for the lower level personnel. The public sector could not offer financial rewards that could attract suitable leaders.

Emergency situations require adapting to varying conditions, developing innovative solutions, and being able to move beyond simple and traditional solutions. In the vernacular of today this is termed “thinking out of the box”. Combined with the political jurisdictional issues, the appropriate leadership for emergency situation may not necessarily be the same as the political leadership. Private sector leaders who advanced in the competitive environment, were successful entrepreneurs, and showed strong survival attributes could be challenged to get involved. Mayor White of Houston, Texas states in chapter 7 that his City did exactly that in the response to the challenges of sheltering thousands of refugees from Hurricane Katrina. The City used successful business and civic leaders to manage provision of certain services. The Mayor created “Virtual organizations.” Specifically, the City set up field hospitals managed by hospitals and pharmacies, enrolled 20,000 evacuated children in schools and raised funds to help students who are behind their grade level, and used hotel and apartment managers to arrange housing for the refugees. A similar effort by Mayor Garrett of the City of Corpus Christi (chapter 8) involved absorption of several thousand of evacuees from Hurricane Katrina, and later the City itself evacuated its own residents and the previous evacuees north to safety. The City government even arranged transportation, and food for the sick and the infirm.

We often witness successful business and corporate leaders turning to politics. Mayor Bloomberg of New York City, Governor Corzine of New Jersey, Governor Shapp of Pennsylvania, Senator Lautenberg of New Jersey, and Governor Romney of Massachusetts are just a few examples. They changed careers and brought private solutions to public problems. Their involvement in government may be motivated by the desire for new challenges in the public sector after having been successful in the private sector. They may also desire the esteem garnered from high level government service and the possibility of further advancement in the political sphere. It has proved to be a win-win situation. The public sector may even enjoy additional financial support from the new political leaders, in addition to their talent and introduction of private management practices into the public sector. Mayor Bloomberg works for \$1 a year. He contributed a new computer system to city government, and his companies provided financial support to community and social groups. Further, high level executives' involvement with the public sector often attracts other private sector younger leaders who wish to be associated with the senior executives.

The private sector executive might well direct all regional homeland security responsibilities, including preparation for and the response and recovery efforts from an event. Preparatory activities are ongoing and include the establishment of a personnel structure and their periodic training, acquisition or emergency drafting of equipment, and development and construction of databases. When a homeland security event occurs, all political jurisdictions and their staffs, including police, fire and ambulance services, come under the control of the director.

A major event requires far more equipment than government normally maintains. This equipment includes fire engines, rescue vehicles, heavy construction type vehicles, medical and other equipment that is event dependent and is difficult to anticipate. Since the private sector owns most of such equipment, we need to develop a process by which equipment could be transferred to the management of the event. The state legislature could grant the homeland security directors the power to requisition with appropriate compensation necessary personnel and equipment from the private sector. Kirschenbaum (chapter 6) reviews the existing Israeli practice where the government requisitions and pays private companies and individuals for using their equipment and buses during emergency situations.

Numerous legal, administrative, and payment issues arise whenever private resources are shifted to the public sector to respond to natural or terrorist events. Responders have to be assured that they will enjoy protection against liability for their interjurisdictional activities performed with usual care and diligence. Prior agreements for private sector resources including personnel and equipment have to be arranged to include their authority, duties, protection against liability, and payments for damages or injuries incurred in the course of their public deployment.

Interstate transfer of resources is more complicated. Public interstate involvement requires the US Congress to approve any interstate compact between states. In the absence of prior agreements, deputizing has to occur before personnel enjoy sovereign immunity. In the aftermath of hurricane Katrina in 2005, Louisiana officials deputized Blackwater security guards who helped patrol New Orleans. The guards were even authorized to use deadly force (Scahill, 2005). Incidentally, similar issues arise when police officers assist from outside the state. Police officers generally have the authority to enforce the state law everywhere within the state.

When the Rita and Katrina natural disasters occurred, the government at all levels encountered difficulties in the prompt delivery of food, water and other emergency supplies to the affected region. At the same time, chain stores had sufficient supplies through use of their normal distribution systems; they transferred supplies from unaffected stores to the stores in the affected region. Also, emergency supplies were even delivered to the New Orleans Dome but could not be distributed because they were unable to gain access. Inventory management including delivery of goods is a normal business function. In preparation for emergencies, the private sector should be contracted to fulfill these functions. Local communities often experience a shortage of supplies after two days of responding to an emergency. Mayor Wallace of Sugar Land, TX (chapter 9) was instrumental in creating the Regional Logistics Center that was managed by a private company. The regional authority in effect established a public-private partnership (PPP) to handle more effectively the management of supplies. The City's leadership was also instrumental in helping to develop a prototype agreement for distant cities to provide aid in emergency situations. The agreement is an attempt to resolve state sovereignty issues that

delayed responses to hurricane Katrina. Baltimore, MD, and Trenton, NJ have such a mutual aid agreement.

Mayor Dellums describes in chapter 10 an interesting PPP that was established to protect the Port of Oakland, CA and its environs. The agreement involves many government and private entities and makes coordinated response and recovery efforts easier. Oakland was instrumental in forming committees along functional and geographical lines and in employing technology like video surveillance around the Port. The unified regional command structure worked well when a ship crashed into a bridge and caused an oil spill.

A form of public-private partnership incorporating volunteers occurred in response to evacuation from hurricane Katrina. Corpus Christi (chapter 8), a city of 285,000, received several thousand refugees from hurricane Katrina. City personnel and volunteers converted the Coliseum for the evacuees, some of whom were sheltered in neighboring communities. Food was provided by volunteer restaurants. Medical services, Internet access and other communications and travel assistance to reunite families were also provided. An emergency operations center and a mobile command post were used. Then, hurricane Rita forced the City to evacuate the refugees and its residents, including, 350 special needs citizens who were transported to a Senior Center and then evacuated to San Antonio. Corpus Christi employees are considered essential and are not allowed to evacuate. The City operated a “refuge of last resort.” Jacksonville, Florida has developed a special needs database so that this group can receive necessary services in a timely fashion (chapter 5). The Special Needs group includes those who are homebound, dependent upon electricity to power oxygen dispensers and other life-saving equipment, or dialysis patients. The City has developed a plan for evacuating special needs individuals to special shelters.

## **5. Establishing Regulated Insurance Programs**

The problem that society faces is that businesses under-invest in protecting themselves against homeland security events. Businesses also under-invest in protecting society against the adverse effects that their actions cause others. We shall outline the reasons for such under-investment,

and suggest how regulated insurance could encourage firms to take more appropriate precautionary measures.

Homeland security incidents, whether natural or terrorist disasters, could be significant in scope and even lead to business bankruptcy with no fault attributable to the individual firm. HLS incidents are uncertain with unknowable probability of occurrence, magnitude and duration of damage which could all lead to the destruction of the firm. There are insurance programs to protect businesses from such events; however, because of the uncertainties involved, premiums are set at high levels by insurers that often deter businesses from subscribing to them. Thus, businesses choose to under invest in protecting themselves against the direct effects on themselves of HLS events.

Firms may also take insufficient HLS precautions that cause adverse effects on other firms. These adverse indirect HLS effects require government intervention to encourage firms to act in a manner that minimizes such effects. Private markets will under-invest in indirect security precautions for the following reasons. First, the adverse effects of an incident are wider ranging than the direct harm to the individual business. Thus, businesses may insure and/or act in order to protect against their own expected suffering without taking account of the indirect adverse effect that the disruption of the business may cause other businesses. Second, a chemical plant may insure and/or take precautions protecting the facility up to its full value. However, a terrorist may steal and use chemicals from the plant to contaminate the entire water supply of the city. We would have liked the plant to take security precautions that significantly reduce the chance of such a theft. Unfortunately the effort is not worthwhile for the plant itself but is desirable for society, considering the expected social costs. Third, the public is not aware whether buildings they visit contain the necessary security in case of an incident. There is asymmetric information because the owner of the building knows the insufficient level of security he/she provides while the “customers” are unaware of the potential danger of working in or visiting the building. Fourth, a company will take precautions to protect its assets up to the value of bankruptcy. The company will not take precautionary actions beyond that level even at a very low cost. However, the social cost of inaction beyond the bankruptcy level may be great and could be avoided at low cost. Fifth, if a company knows that the government will

compensate businesses in case of a disaster, it will take no or a low level of necessary security precautions. For example, buildings may be designed and built to sustain an earthquake but since the company expects the government to compensate victims in case of such disaster, the company will not spend the additional money to improve the sustainability of the building. All these points suggest government intervention to achieve socially desired level of precautions (above discussion is based on Orszag, 2003). There are also the market failure issues emanating from the short-term interest of corporate managers.

The problem of negative externalities caused by under investment in security is similar to the environmental issue of controlling pollution (Auserwald, 2005). The solution suggested by economists and implemented by governments involved introducing direct regulation and then market-based auctioning to regulate the amount of allowed pollution. Government regulation was necessary because the adverse effects often occur after many years and their causes cannot be attributed to individual firms. In the case of under investment in security that causes social costs to other agents, the effect is immediate and the link to the responsible firm can be more easily identified. Thus, reliance on markets and individual HLS insurance is appropriate.

It is obvious that markets are inefficient with regard to uncertain substantial homeland security events. In order to correct the under-investment, government intervention could take the form of regulation, required insurance, or subsidization of security precautions. Government intervention in this case is aimed at correcting for both the inadequate amount firms spend for a HLS event and the amount needed to correct or avoid the external or spillover negative effects

An important criterion in evaluating the above three alternatives is to select the one that requires minimum government intervention in this marketplace. Insurance is the least intrusive and allows the most opportunities for market forces. But, some regulation is often necessary to take account of asymmetric information or to assure minimum standards of security. For example, regulation may appropriately specify armed guards for nuclear facilities. Subsidization of businesses for undertaking appropriate security precautions has all the usual shortcomings of encouraging unnecessarily expensive investments, sparking lobbying to obtain the subsidy,

providing funds for activities that might be taken in any event, and causing undesirable distributional consequences (Orszag, 2003: 9).

Through requiring insurance market forces are unleashed to encourage a more efficient investment in precautionary efforts. There are numerous insurers, and all businesses will be required to obtain HLS insurance. Thus, a competitive market will develop, and insurers should earn close to normal profits. Depending upon the specifications of the regulation, a monopolistically competitive market is expected where insurers will offer various policy packages to businesses. Businesses will have the option of paying lower premiums and spending more and/or undertaking greater precautionary efforts. Or, alternatively businesses can pay greater premiums and take fewer precautions. Businesses will select the least cost option, a situation which is socially desired.

Before 9/11 there were few companies that insured against acts of terrorism and the premiums were quite modest. For example, before 9/11 O'Hare airport in Chicago had \$750 million in terrorism protection for an annual premium of \$125,000. After 9/11, O'Hare could only obtain \$150 million of coverage for \$6.9 million per year. In fact, prior to 9/11 terrorism protection was usually included within normal commercial insurance. However, soon after 9/11, most policies, including worker's compensation, excluded terrorism protection so that by September 11, 2002, very few companies had terrorism insurance (Kunreuther and Michel-Kerjan, 2004: 203).

Since 1996 catastrophe bonds have been used in the U.S. to defray part of the risk of insurance losses from natural disasters. They yield higher than normal interest. However, if a natural disaster occurs, either the principle or the interest payments cease depending on the specifics of the bond. To date, they have not been used in the terrorism realm.

The magnitude of potential losses is another issue. Hurricane Andrew which occurred in 1992 had insured losses of \$19.6 billion in 2001 dollars. The insured losses in the 9/11 attack, the largest catastrophe in US history, amounted to \$30-70 billion (Joint Economic Committee, 2002:1). As of May, 2007, the Insurance Information Institute (May, 2007) reported that total insurance claim payments were \$35.9 billion. The total surplus of the insurance industry in 2001

was somewhere between \$300 billion, and \$427 billion. But the surplus associated with or available to pay high risk commercial targets in 2001 was only \$100 billion. Thus, 9/11 consumed about One third of the relevant insurance industry surplus. All other attacks were much smaller in magnitude; the first World Trade bombing and the Oklahoma City bombing had, respectively, insured losses of \$725 million, and only \$145 million. The Joint Economic Committee of the US Congress concluded that the insurance industry could pay the 9/11 claims but the payments will significantly impair the industry ability to withstand another catastrophe (Joint Economic Committee. 2002:3).

Following 9/11, \$22 billion of the \$33 billion were paid by reinsurance companies (Auerswald, 2005). The high cost and the uncertainty then led these companies to cease offering terrorism coverage. Accordingly, since 2002, the federal government has had a program to cover insurance companies' losses in case of a terrorist attack. The provisions of the program have increased the portion that insurance companies must bear before the federal program comes into play.

In 2007, the US Government would underwrite 85 percent of insurance companies' losses emanating from a terrorist act in excess of 20 percent of insurance companies' premiums. The federal government underwrites up to \$100 billion above the \$27.5 billion that insurers will spend. The insurance companies must then pay a surcharge not to exceed 3 percent for premiums covered by the Terrorism Risk Insurance Act and its extension (TRIEA) to reflect government exposure. The provisions are similar to those of Great Britain whose program has been in effect since 1993. Insurance companies must now bear a larger portion of the damages before the federal program coverage begin. Clearly, if a company does not carry terrorism insurance it does not receive any government support. In spite of reserves that seem adequate, we witness here a market failure that seemingly requires government underwriting of catastrophic HLS events. The impact on the overall economy of a catastrophic event helps justify such government involvement.

It is noteworthy that indirect business losses to non-direct victims are not covered unless specifically included in the terms of the insurance policy. A federal district court in Chicago has

held that O'Hare Airport was not entitled to compensation under its terrorism insurance policy as a result of 9/11 when all flights were grounded by order of the F.A.A. and therefore the Airport incurred substantial losses (City of Chicago, the Factory Mutual Insurance Co., 2004). This is the standard legal interpretation of insurance policies where direct victims are fully covered but indirect victims are not covered for their business losses. A business would seem to be better off being a direct victim than being an indirect victim.

If a HLS event occurs then some suggest that government should step in and help businesses survive. Relief from an event and recovery efforts appear to be "public goods" because of the spillover effects on society. However, some may claim that it is not the role of government to rescue businesses. Also, if government is expected to help in the aftermath of major HLS events, there is little incentive for businesses to take precautions in advance to prevent such major harms. Businesses should know for certain that either government will not aid them or know the extent of aid in the aftermath of devastating events. In any case, the objective is to avoid a collapse of the economy emanating from a major terrorist event. Federal compensation is designed to prevent devastating negative social externalities caused by the attack. For example, the Federal Reserve provided billions to rescue Bear Sterns whose failure would have threaten to collapse the financial system in the wake of the subprime fiasco.

## **6. Employing Technology**

Technology improvement is crucial for the four categories of gathering intelligence, preventing attacks and natural disasters, responding to events, and recovering from them. Correspondingly, technology is used for data mining in order to detect irregularities; digital cameras with face recognition can observe known terrorists. Computer assisted systems can help to manage an event and the recovery efforts. Intelligence gathering through data mining is done mainly by the federal government with some intelligence work done by state governments. State and local governments are establishing emergency centers where all relevant services are located during disaster situations and where communication channels are provided to the field forces.

The question in the area of investment in technology is whether the allocation of spending for the four categories is efficient. Economists claim that efficient use of resources requires that the last dollar spent on each category yields the same benefit. Even if we spend the right amount on each category, it is still uncertain whether resources are spent on the right type of technology and at the appropriate time.

These allocation problems always exist. However, where governments are the primary decision makers the appropriateness question is exacerbated. Government lacks the profit motive which guides business in the decisions about which technology to adopt and when. In private markets prices and inherent demands provide signals to producers about the appropriate rate and direction of innovative activities. These signals are lacking in the homeland security field. Government often is unaware of products that might improve security and lacks channels to communicate needs to technology companies. When developing or even contemplating developing security products, technology companies have limited knowledge of government needs because of perceived conflict of interest issues. It is important to maintain forums at which government and private technology personnel interact. Under existing conflict of interest regulations, such forums could be convened by neutral entities like universities.

Information gathering using technology includes data mining, digital cameras, fusion centers, improved telecommunications, and the use of the Internet to transmit the information. Governor Ehrlich of Maryland outlines in chapter 11 the creation of a fusion center that collects information from all sources and mines the data in order to detect irregularities that suggest terrorist activities. The public is encouraged to provide information through a “tip line.” The Center has federal, state, local, and private sector participation representing 250 agencies or organizations. A principle objective of a fusion center is to develop a pattern of cooperation and information sharing. Governor Rendell of Pennsylvania (chapter 12) created a unified database for criminal, judicial and corrections which is being expanded to include HLS usage and information from federal, state, local and adjacent states. First responders will have access to the information. In chapter 13 we learn from Governor Minner of Delaware about the fusion center that started operation in 2005. It is unusual because law enforcement members are joined by agricultural, transportation, and health experts, the National Guard and other governmental

agencies. The fusion center has a “tip line” and is helped by the uniform reporting system employed by all the law enforcement agencies in the State. The Center was instrumental in de-escalating the action plan by fusion Center stakeholders after a 2004 crash of a U.S. Air force C-5 transport plane.

Mayor Pringle of Anaheim, CA (chapter 14) created a virtual operations center to manage emergency situations. Authorized users could now manage events from any computer. It has a landing page where users can access information ranging from building blueprints to traffic flow around the incident. Regional communities also participate in the virtual center. The system has worked well in the case of fires and in a simulation of a major disaster.

Cameras deployed throughout a jurisdiction could help gather information. The data are mainly used for operations but they could be used for data mining. Bellwood, Illinois in 2005 (chapter 15) created an integrated wireless surveillance network focused on 2.5 miles of public streets, sidewalks, and alleys. The system has both audio and video and can focus on sounds of breaking glass or gunshots. Cameras were also installed at intersections to catch red light runners, illegal right on red turns, violators of railroad crossing signals, and even overweight trucks. The system has reduced 911 calls for service, and such property crime as auto theft. Bellwood also instituted a wireless communications system that allows data, pictures, and other information to be provided to officers on patrol and fire fighters in transit to an emergency. The sophisticated system allows personnel to view traffic cameras so they can often determine the situation before arriving on the scene. Intelligent cameras are already being used elsewhere for surveillance with facial recognition, and some can identify suspicious objects through quasi x-ray ability. When the cameras detect any such elements, an alert is generated.

Adequate communications are necessary for effective rescue operations. Rescue efforts on 9/11 were impeded when the cellular antennas at the top of the Twin Towers collapsed. Access calls are usually diverted to other antennas but the magnitude of the calls caused a collapse of the entire cellular system. Thus, rescue efforts relied more on personal contacts and with the leaders “on the scene” than on communication systems. Collier County, Florida experienced similar communication problems during hurricanes Charlie and Wilma. Disruptions occurred in the

public switched network, the cellular systems, and the Internet. In response to that experience, chapter 16 by Collier County officials James Mudd and Barry Axelrod reports on its improved public safety system. The County added more automotive radios which are less reliant on antennas, developed a private optic data network, improved the connectivity between the private data network and the internet, and improved the telephone system through reduced reliance on one central office. It also enlisted volunteers who are “ham” radio users to provide communication during an emergency. The latter are least dependent on any infrastructure and therefore their communications are robust. Mayor Cicilline of Providence RI states in chapter 17 that his city was one of the first cities to make data in a digestible form available to field officers. The officer in the field has information equivalent to that at the station and can complete reports that enter the database. The internet is making such practice commonplace.

The lack of interoperable communications between the police and the fire forces contributed to the loss of lives of responders. Interoperable radio communication is the solution promoted and funded by the federal government. The failure of the communications and the lack of interoperability have also been dominant themes raised by governors and mayors. To achieve interoperability the federal government supports state and local governments by grants of around \$2.7 billion. Governor Round and Otto Doll of South Dakota report on how a statewide radio system was developed that allows its more than 14,000 public safety officials (local, state, federal, and tribal) to communicate with each other. The digital, trunked system permits voice and data transmission in a cost-effective manner. The trunked feature ensures efficiency because the computer searches to find the first available channel rather than dedicating a particular channel to a particular user. Tacoma, Washington (chapter 19) established a region-wide cooperative effort to promote, evaluate, implement, and manage technology applications for law enforcement. The technology incorporates police, HLS, and the courts under one organization where relevant data are maintained, evaluated, and distributed to the appropriate law enforcement agencies. Mayor Will Wynn of Austin, TX describes in detail in chapter 20 the history and process of integrating the communication systems in the region. In chapter 21, Mayor Iorio of Tampa outlined the development of a regional cooperative, interoperable police, fire, and emergency management systems and a joint operations center where each maintains its own system to satisfy special requirements.

The communications policy has not been free of controversy. In a testimony before US Congress, one expert stated that not every firefighter or police officer needs an interoperable radio. Only those actually at the scene should be so equipped. A simple mobile interoperable communication system at the scene valued at merely a million dollars will suffice. Only a few such systems need to be purchased by each major city (O'Hanlon, 2007). This suggests possible over spending on technology. Further, political issues enter into the allocation of government funds. For example, rural states like Wyoming or Montana have received larger per capita homeland security funds, including presumably communications grants, than major cities like New York and Washington that are prime targets for terrorist attacks.

Emergency operations centers have an interesting history. Former New York Mayor Rudolph Giuliani completed in 2000 his innovative emergency center at the Twin Towers in the financial district of the City. The Center also had a conference room for all the commissioners and the Mayor. The Center was used a few times for specific emergency situations like water breaks, and electricity shutdowns. The Center became the emergency operational facility where critical city and public utilities migrated during a crisis. In a disaster, all phone lines are diverted to it. The Center's location at the Twin Towers was decided after a thorough analysis of various locations in the city. It was determined that only a direct atomic bombing of the building could endanger the center. Unfortunately, no one could have predicted the vicious attack on the Twin Towers that prevented its use at the most critical time of that attack. Incidentally, an emergency center does not normally perform data mining and the opposite is also true.

Many other cities followed NYC's project while employing new technologies that became available. Washington D.C. under Mayor Williams (chapter 22) has developed innovative technologies for homeland security. The improvements included the establishment of a command center that is in operation at all times. It has the capability for voice, video, wideband and wireless communications. Remote back up capability was created. Interestingly, the Center was located in an economically deprived section of the city in part to stimulate the area's development. The technology allows viewing activities throughout the city, adjusting traffic

patterns, and the deployment of forces. The Center was used to control major events like July 4<sup>th</sup> celebrations and the 2005 Presidential Inauguration.

Chicago under the leadership of Mayor Daley (chapter 23) developed a Joint Operations Center which brings together in one room federal, state, municipal, and utility emergency personnel to monitor and react to events like storms, utility interruptions, and terrorist attacks. Digital cameras are monitored at the Center. Detailed digital floor plans of all tall building and major infrastructure are available on the Center's computers. Chicago also has a mobile unit that can perform all the functions of the Joint Operations Center. This unit which could serve as a backup Center can be dispatched to the place of an incident and would prevent the situation of 9/11 in NYC where the Center was destroyed. Chicago employed the mobile unit to handle successfully the 2007 New Year's celebration which occurred at the same time as a major playoff football game.

Virginia (chapter 24) developed and implemented a continuity of operations plan for all disasters including a possible flu pandemic. Continuity plans include provision for use of alternative facilities in case a disaster disables the primary department or agency facility. Virginia also created a new Emergency Operations Center with sufficient space to accommodate individual departments and agencies that have had their facilities made inoperable. The Emergency Operations Center has sophisticated computer and communications technology which permits operational management of a disaster. Especially important is the redundancy aspect so that the Center is resilient to failure of any individual system.

The human element and the specific culture of the targeted population are most important for successful implementation of technology in homeland security. Morales and Ramsey argue in chapter 25 that the IT people are important in educating other members of the organization.

## **7. Conclusions**

Since 2001, government at all three levels face increased demand for homeland security services that could be partially met through restructuring of existing emergency services, shedding non-public services, and contracting out public good services. Homeland security services include

preparation and training for anticipated events, and assisting in satisfying the unknowable peak load demand. We suggested ways to engage the private sector in preparing and providing homeland security services before and during such events. We also suggested requiring insurance against catastrophic events that will encourage businesses to take appropriate security precautions. Technology is often an efficient substitute for labor. However, since government is not motivated by profit and the social net benefits are unknowable, the appropriate technology may not be developed or deployed. Governments could either over or under spend on technology for homeland security.

Specific recommendations include verified response to false alarms for police, and charging prices that cover the long run avoidable cost for fire and ambulance response to false calls. Shedding non-public police services like animal control, escorting funerals, and unlocking cars. We suggest establishing reserve units for homeland security. Private security guards and directors will be trained and deployed to pre-assigned obligations in case of an event. Retired emergency services' officers could also be invited to join such a force. Personnel should be paid for the time they serve on the force. We also suggest that the commanding officers could be police chiefs or private executives who volunteer. Private executives are often interested in public service and obviously have the requisite managerial and entrepreneurial skills. Finally, our suggestions for public-private partnerships are consistent with the current emphasis of expanding the role of the private sector in providing public services.

Improving homeland security in the public sector will probably encounter a few problems. Several years have passed since 9/11, and no other terrorist attacks occurred within the US. It may become difficult for elected public official to justify local and state spending on homeland security. This excludes activities related to natural disasters. It is more popular to exhibit achievements in services that contribute directly to the constituents. Besides, the public expects the federal government to cover all defense and homeland security expenses.

In the background section, we discussed the asymmetric information problem where the terrorist has the freedom of choosing the target, the timing, the nature and extent of an attack. Public budget constraints make target hardening in the form of prevention activities thin and ineffective

across the many critical infrastructures. One solution is to maintain limited personnel at most facilities and employ technological advanced sensors to alert and provide necessary information about attacks. Obviously, high risk targets like nuclear plants require strong security measures. Most of the financial resources should be spent on effective response and recovery efforts. Another possible preventive measure is to respond by randomly securing most critical infrastructures. Thus, the policy might be to respond in a random fashion to the terrorist, creating uncertainty on their part.

The other problem relates to the lack of incentives to promote managerial and technological innovations in the public sector. Unions of public employees often object to merit or incentive payments, preferring across the board increases in compensation. Encouraging innovations including obtaining patents, however, requires significant financial incentives. State and local governments have technology experts working at the IT and the homeland security departments and in other security related departments. State and local governments could establish incentive systems.

Ordinary disasters have been and are successfully managed by state and local governments. National homeland security efforts should mainly address major catastrophic events that could occur in various locations in the US. For example, a terrorist attack that might simultaneously destroy sewer facilities in many metropolitan areas or a major natural disaster might affect many states. Society has to prepare for a low probability event that could have significantly large adverse effects. The US has enough emergency resources to handle almost any event; it is basically an issue of peak time demand where the existing resources must be mobilized to confront the calamity with minimum disruption. We suggest establishing public-private partnerships that will prepare and train for such an event and where private resources could be added to the existing public emergency resources. Thus, an appropriate role for the US DHS or the National Governors Association would be to induce states to establish regional compacts to share governmental resources while incorporating private resources and private sector ideas. The objective is to mobilize emergency resources from non-affected areas and from the private sector to assist the impacted area. We are optimistic that unleashing the private sector will help minimize the disruption from any natural or terrorist attacks.

## 8. References

Auerswald, Philip et al (2005). “The Challenge of Protecting Critical Infrastructure”, **Issues in Science and Technology**, fall. Obtained from <http://www.issues.org/22.1/auerswald.html>. Last accessed September 19, 2008.

Blackstone, Erwin A., Andrew J. Buck, and Simon Hakim (2007). “The Economic of Emergency Response”, **Policy Sciences**, Vol. 40 (4): 313-334).

Blades, Marleah (2008). “Helping Hands: The FBI is working with the Private Sector to Enhance Corporate Security and to Promote National Security”. **Security Technology and Design**, May: 36-38.

Bureau of Justice Assistance (BJA) (2005). **Engaging the Private Sector to Promote Homeland Security: law Enforcement-Private Security Partnerships**, US Department of Justice, Office of Justice Programs, NCJ 210678, September.

City of Chicago v. factory Mutual Insurance Co., 2004 U.S. District Lexis 4266.

Clarke, Richard A. Rand Beers, et al. (2006). **The Forgotten Homeland: A Century Foundation Task Force Report**, the Century Foundation, New York, NY.

Council of Foreign Relations (2003). **Emergency Responders: Drastically Underfunded, Dangerously Unprepared**. The Rudman Report, NY, NY.

Critical Infrastructures, 2008. “Chemical plants-go well beyond well prepared”, **Newsweek**, November 5, 2001. Obtained from [www.newsweek.com/id/76228/page/1](http://www.newsweek.com/id/76228/page/1) Last visited 9/16/2008.

[www.apwa.net/Advocacy/Infrastructure](http://www.apwa.net/Advocacy/Infrastructure) Last visited 9/16/2008

[www.fpl.com/environment/nuclear\\_power\\_serves\\_you.shtml](http://www.fpl.com/environment/nuclear_power_serves_you.shtml) Last visited 9/16/2008.

Flynn, Stephen (2007). **The Edge of Disaster: Rebuilding a Resilient Nation**. Random House, New York.

Insurance Information Institute (2007). “9/11 and Insurance: The Five Year Anniversary”, New York, NY, available from [www.iii.org](http://www.iii.org). Last accessed May 19, 2008.

Hakim, Simon, Andrew J. Buck, and Erwin A. Blackstone (2007). “Funding the Local War on Terror”, **Milken Institute Review**, Vol. 9 (1), First Quarter: 46-56.

Joint Economic Committee of the US Congress (2002). “Economic Perspectives on Terrorism Insurance”, May.

Kunreuther, Howard and Erwann Michel-Kerjan (2004). “Challenges for Terrorism Risk Insurance in the United States”, **Journal of Economic Perspectives**, Vol. 18 (4), fall: 201-214.

Office of Management and Budget (2008). **Analytical Perspective on the Budget of the US, Fiscal Year 2008**. Obtained from [www.whitehouse.gov/omb/budget/fy2008](http://www.whitehouse.gov/omb/budget/fy2008).

O’Hanlon, Michael, 2007. “A Broad Take on America’s Current Homeland Security”, Testimony before the House Committee on Homeland Security’s Subcommittee on Border, Maritime and Global Counterterrorism, March 8.

Orszag, Peter E. (2003). “Homeland Security and the Private Sector”, Testimony before the National Commission on Terrorist Attacks Upon the United States, November 19.

Scahill, Jeremy (2005). “Blackwater Down”, in **The Nation**, October 10. Visited <http://www.thenation.com/doc/20051010/scahill> Visited May 6, 2008.