VIEWING URBAN DISRUPTIONS FROM A DECISION INFORMATICS PERSPECTIVE

James M. TIEN

Rensselaer Polytechnic Institute
Troy, New York, USA
tienj@rpi.edu

Abstract

Urban infrastructures are the focus of terrorist acts because, quite simply, they produce the most visible impact, if not casualties. While terrorist acts are the most insidious and onerous of all disruptions, it is obvious that there are many similarities to the way one should deal with these willful acts and those caused by natural and accidental incidents that have also resulted in adverse and severe consequences. However, there is one major and critical difference between terrorist acts and the other types of disruptions: the terrorist acts are willful – and therefore also adaptive, if not coordinated. One must counter these acts with the same, if not more sophisticated, willful, adaptive and informed approach. Real-time, information-based decision making – which Tien (2003) has called the decision informatics paradigm – is the approach advanced herein to help make the right decisions at the various stages of a disruption. It is focused on decisions and based on multiple data sources, data fusion and analysis methods, timely information, stochastic decision models and a systems engineering outlook; moreover, it is multidisciplinary, evolutionary and systemic in practice. The approach provides a consistent way to address real-time emergency issues, including those concerned with the preparation for a major disruption, the prediction of such a disruption, the prevention or mitigation of the disruption, the detection of the disruption, the response to the disruption, and the recovery steps that are necessary to adequately, if not fully, recuperate from the disruption. The efforts of the U. S. Department of Homeland Security and its academically-based Homeland Security Centers of Excellence are considered within the proposed types, stages and decisions framework.

Keywords: Data fusion, data analysis, adaptive algorithms, decision modeling, systems engineering

1. Introduction

Urban infrastructures are the focus of terrorist acts because, quite simply, they produce the most visible impact, if not casualties. From the September 11, 2001 (i.e., "9/11") attack on New York City's World Trade Center to the more recent March 11, 2004, attack on Madrid's commuter trains, it is obvious that urban centers are indeed vulnerable to such hideous acts. A systemic or holistic approach to securing the infrastructure systems that underpin an urban center is

ISSN 1004-3756/05/1403/257
CN11-2983/N ©JSSSE 2005

JOURNAL OF SYSTEMS SCIENCE AND SYSTEMS ENGINEERING
Vol. 14, No. 3, pp257-288, September 30, 2005

required. New York City (NYC), for example, is not only an obvious target of terrorism; it is also a major urban center, with all the attendant complexities of people, processes, products, physical structures and institutions. As a consequence, NYC – and its symbolic World Trade Center – was an obvious target for the 9/11 terrorists, whose colleagues had previously targeted the same symbolic structure back in 1993.

While terrorist acts are the most insidious and onerous of all disruptions, it is obvious that there are many similarities to the way one should deal with these willful acts – which would also include a malicious prankster releasing an electronic virus on the Internet – and those caused by natural and accidental incidents that have also resulted in adverse and severe consequences. Indeed, the natural disasters of droughts, diseases, floods and earthquakes – including the 1899-1901 drought in India, the 1917-1919 world-wide influenza epidemic, the 1931 Hwang-Ho flood in China, and the 2004 Tsunami in South Asia – have been the scourge of mankind. Fortunately, accidental disruptions (e.g., asbestos contamination, carcinogen exposure, oil spills, power failures, and nuclear accidents) have thus far been less disastrous, but they may begin to rival the natural disasters in impact as one explores the potentially high-payoff but equally high-risk worlds of nanotechnology and biotechnology. Nevertheless, the public expects that the accidental hazards can and should be fixed as they are man-made; on the other hand, natural hazards are considered to be acts of God whose negative effects can only, at best, be mitigated. However, there is one major and critical difference between terrorist acts and the other man-made but accidental disruptions: the terrorist acts are willful – and therefore also adaptive, if not coordinated. Since terrorist – and other willful (e.g., electronic viruses, hacker attacks, and email spam) – acts are based on the most up-to-date intelligence or information, one must also counter these acts with the same, if not more sophisticated, willful, adaptive, coordinated and informed approach.

More specifically, the approach of real-time, information-based decision making – which Tien (2003) has called the decision informatics paradigm – is focused on decisions and based on multiple data sources, data fusion and analysis methods, timely information, stochastic decision models and a systems engineering outlook. It should be emphatically stated that while the terms employed in describing the methodologies that underpin decision informatics are those belonging to decision analysis (i.e., emergency management, statistics, risk analysis, etc.), decision informatics is clearly multidisciplinary in nature and, depending on the problem being considered, could include experts from science (i.e., information, visualization, cognition, sociology, etc.), engineering (i.e., telecommunications, biomedical, chemical, nuclear, etc.) and other disciplines (i.e., religion, theology, terrorism, culture, etc.). It provides a systematic and consistent way to address real-time emergency issues, including those concerned with the preparation for a major disruption, the prediction of such a disruption, the prevention or mitigation of the disruption, the detection of the disruption, the

response to the disruption, and the recovery steps that are necessary to adequately, if not fully, recuperate from the disruption. More importantly, one must approach an urban emergency management problem in a systemic or holistic manner, especially given the interdependencies of the underlying infrastructure systems.

Although the focus of this paper is primarily on terrorist disruptions, it is obvious that the decision informatics approach is likewise applicable to the preparation, prediction, prevention, detection, response and recovery steps associated with the emergency management of any major urban disruption. The remaining sections of the paper deal with the types of disruption, the stages of or life cycle in a disruption, the decision informatics paradigm, and the combination of types, stages and decisions in regard to the efforts of the U. S. Department of Homeland Security and its academically-based Homeland Security Centers of Excellence, followed by some concluding remarks.

2. Types of Disruptions

Modern society relies on the reliable operation of a set of human-built systems – each being a combination of people, processes, goods, services, physical structures and institutions – to sustain people themselves, infrastructures and commerce. In an urban center, these human-built or constructed systems include transportation (i.e., roads, bridges and rail); health (i.e., clinics, emergency rooms and hospitals); education (i.e., pre-college, college and continuing education); energy (i.e., electric power, gas and liquid fuels); telecommunications (i.e., radio, telephone and internet); information technologies (i.e., file servers, database systems and networks); water (i.e., lakes, reservoirs and rivers); food (i.e., farms, markets and warehouses); sanitation (i.e., garbage, sewage and air pollution), structures (i.e., homes, buildings and spaces); civil order (i.e., police, fire and health); finance (i.e., banks, insurance and security firms), and government (i.e., local, state and federal). People, infrastructures and commerce all rely on the constructed systems to provide the necessary goods and services.

In the U. S., the constructed systems – most of which are privately owned and operated – are so essential that they have been called the nation's "lifelines" and are included in the broader set of critical infrastructures defined by the President's Council on Critical Infrastructure Protection (PCCIP) (U. S. President, 1998) to be those physical and cyber-based systems essential to the minimum operations of both the economy and the government. More specifically, the U. S. National Strategy has identified 14 sectors – agriculture (2M farms), food (90K food-processing plants), water (2K federal water reservoirs), public health (6K registered hospitals), emergency services (90K emergency service entities), government, defense industrial base, information and telecommunications (2B miles of telecom cable), energy (3K electric power plants, 2M miles of pipelines), transportation (5K public airports, 120K miles of major railroads, 590K highway bridges), banking and finance (27K banking and financial institutions), chemical

industry and hazardous materials (66K chemical plants), postal, and shipping – and 5 key resources – national monuments and icons, nuclear power plants (104 commercial nuclear power plants), dams (80K dams), government facilities (3K federal facilities), and critical commercial assets (0.5K skyscrapers) – that must be protected.

Historically, the nation's critical infrastructures have been physically and logically separate systems that had little interdependence. However, as a result of advances in information technology and the necessity for improved efficiency and effectiveness, these infrastructures have become increasingly automated and interlinked. In fact, because the information technology revolution has changed the way business is transacted, government is operated, and national defense is conducted, the U. S. President (2001) singled it out as the most critical infrastructure to protect following 9/11. Thus, while the U. S. is considered a superpower because of its military strength and economic prowess, non-traditional attacks on its interdependent and cyber-supported infrastructures could significantly harm both the nation's military power and economy. Clearly, infrastructures, especially the information infrastructure, are among the nation's weakest links; they are vulnerable to willful acts of sabotage. The U. S. National Academies' Committee on The Role of Information Technology in Responding to Terrorism (2005) has made a number of recommendations to reduce vulnerabilities associated with the information infrastructure, including undertaking more research in authentication, detection, containment and recovery.

The infrastructure interdependencies are most obvious when a disruption occurs. For example, interruptions in power and communications following the 9/11 attack, in turn, forced the closing of the New York Stock Exchange, which is a critical part of the nation's banking and finance infrastructure. As another example, the August 2003 electrical power outage on the east coast caused the failure of wireless communications and affected the City of Cleveland's water system. Clearly, there are innumerable interdependencies among the various infrastructure networks or systems that provide for a continual flow of goods and services essential to the defense and economic security of a nation. Indeed, for this reason, it is inappropriate to only categorize some infrastructure systems as being critical; they are all critical to the proper functioning of a nation or urban center – otherwise, the non-critical ones might well become the weakest links and thus vulnerable to attack and destruction. More importantly, the infrastructure interdependence problems should not be minimized, especially from a security and reliability perspective; in fact, contingency plans or backup systems should be developed and employed to mitigate these problems.

Sadly, the same advances that have enhanced interconnectedness have created new vulnerabilities, especially related to equipment failure, human error, weather and other natural causes, and physical and cyber attacks. Thus, electronic viruses, biological agents and other

toxic materials can turn a nation's "lifelines" into "deathlines" (Beroggi and Wallace, 1995), in that they can be used to facilitate the spread of these materials – whether by accident or by willful act. Even the Internet – with almost a billion users – has become a terrorist tool (Talbot, 2005); jihad websites are recruiting members, soliciting funds, and promoting violence (e.g., by showing the beheading of hostages). Also, as evidenced by the 9/11 attack, components of an infrastructure system can be used as weapons of destruction. Further, the built environment is often the battleground for engaging the threat or disruption and its impact. Office buildings, subways, airports, water pipes, and power-generation and transmission facilities are all possible targets for terrorist acts, resulting in fires, toxic materials, debris and flooding.

As identified earlier, there are, in essence, three types of disruptions: those natural incidents due to nature and/or natural forces; those accidental incidents due to human errors and/or structural failures; and those willful incidents due to human acts and/or destructive weapons. The who, what, when and where of a number of well known disruptions occurring in the latter half of the 20th century are considered in Table 1 – they include natural disasters caused by the 1969 Hurricane Camille, the 2002 SARS Epidemic, and the 2004 South Asia Tsunami; accidental tragedies due to the 1984 Bhopal Gas Tragedy, the 1986 Chernobyl Nuclear Disaster, and the 1989 United 232 Explosion; and willful acts carried out in the 1993 Oklahoma City Bombing, the 1995 Tokyo Subway Attack, and the 2001 9/11 Tragedy. Several of these disruptions (i.e., Bhopal, United 232, Oklahoma City, and Tokyo Subway) are further considered in Larson et al. (2004), especially in regard to lessons learned.

More recently, the Office of State and Local Government Coordination and Preparedness of the U. S. Department of Homeland Security (2005) provided 15 plausible disruption scenarios that could be used for planning purposes and that could help focus the allocation of billions of federal dollars which will be distributed in the future to help secure the homeland. More specifically, 12 of the scenarios pertain to willful terrorist acts and include: a nuclear detonation of a 10-kiloton device, a biological attack with aerosolized anthrax spray, a biological attack through release of pneumonic plague, a chemical attack with aerosolized chemical blister spray, a chemical attack through explosion of toxic chemical cargo, a chemical attack through release of sarin gas in ventilation systems, a chemical attack through explosion of chlorine gas storage tanks, a radiological attack with radioactive cesium-137 bombs, an explosives attack with handmade bombs or suicide belts, a biological attack through contamination of food items with liquid anthrax, a biological attack through infection of farm animals with food-and-mouth disease, and a cyber attack on the nation's financial infrastructure. The remaining three scenarios concern natural disasters and include: a biological disease outbreak like an influenza pandemic, a 7.2-magnitude earthquake on a fault line through a major urban center, and a category 5 hurricane with sustained winds of 160 miles per hour and storm surges of 20 feet hitting a major metropolitan area.

Table 1 Example Disruptions

Description	Nature of Disruption			
	Who?	When?	What?	Where?
❖ **Natural**				
❖ 1969 Hurricane Camille	❖ Category 5 (out of a possible 5) hurricane.	❖ 2 AM, August 17, 1969.	❖ Regional: 255 killed; thousands evacuated; $4.2B damage.	❖ Makes landfall along Mississippi coastline.
❖ 2002 SARS (Severe Acute Respiratory Syndrome) epidemic	❖ Employing DNA sequencing information, SARS was identified in 24 hours as a coronavirus strain from wild animals, including poultry.	❖ November, 2002—July, 2003.	❖ Worldwide: 774 killed; 7,322 injured.	❖ Began in South China, then Canada and Southeast Asia plus a few cases in Europe and U.S.
❖ 2004 South Asia Tsunami	❖ Magnitude 9.0 Indian Ocean earthquake causing tsunami tidal waves of up to 50 feet high.	❖ 8 AM, December 26, 2004.	❖ Regional: over 160K killed; thousands injured; millions displaced.	❖ Affecting Indonesia, Sri Lanka, India and Thailand.
❖ **Accidental**				
❖ 1984 Bhopal Gas Tragedy	❖ Toxic methylisocyanate chemical vapor escaped from Union Carbide plant due to safety valve malfunction.	❖ 11 PM, December 2, 1984.	❖ Regional: Over 10K killed; over 0.5 million injured.	❖ Small town of Bhopal, India.
❖ 1986 Chernobyl Nuclear Disaster	❖ While testing Reactor 4 and ignoring safety procedures, a chain reaction caused explosion and release of highly radioactive material.	❖ 1 AM, April 26, 1986.	❖ Regional: 31 immediately killed; thousands injured and suffering disease; millions affected by remaining radiation.	❖ Chernobyl nuclear power plant consisting of 4 reactors located in the Ukraine.
❖ 1989 United 232 Explosion	❖ Failure of all 3 hydraulic flight control systems of Northwest's DC-10.	❖ 3 PM, July 19, 1989.	❖ Local: 186 (out of 300) crew and passengers killed; many injured.	❖ Plane crash lands on runway in Sioux City, Iowa.
❖ **Willful**				
❖ 1993 Oklahoma City Bombing	❖ Timothy McVeigh and others built bomb that was placed in a rented Ryder truck.	❖ 9 AM, April 19, 1993.	❖ Local: 168 killed, hundreds injured; building destroyed.	❖ Oklahoma City Alfred P. Murrah Federal Building.
❖ 1995 Tokyo Subway Sarin Attack	❖ Members of terrorist group attacked 5 subway lines leading to center city with toxic sarin nerve gas.	❖ 8 AM, March 20, 1995.	❖ Local: 12 killed, thousands injured.	❖ Subway cars in Tokyo, Japan.
❖ 2001 9/11 Tragedy	❖ 19 terrorists took over 4 airliners, each loaded with thousands of gallons of jet fuel, and crashed them into highly visible U.S. targets.	❖ 8:47 AM—10:06 AM, September 11, 2001.	❖ Local: 3000 killed; billions of dollars of infrastructure and commercial damage.	❖ American 11 crashes into World Trade Center (WTC) north tower; United 175 crashes into WTC south tower; American 77 crashes into Pentagon; United 93 crashes in field near Shanksville, PA.

Table 2 Disruption Characteristics

Characteristics	Types of Disruption		
	Natural	Accidental	Willful
Cause:			
❖ Primary	❖ Nature	❖ Human Errors	❖ Human Acts
❖ Secondary	❖ Natural Forces	❖ Structural Failures	❖ Destructive Weapons
Onset:			
❖ Period	❖ Hours/Days	❖ Hours	❖ Minutes
❖ Predictability	❖ High	❖ Medium	❖ Low
❖ Adaptability	❖ Low	❖ Low	❖ High
Target:			
❖ Primary	❖ Infrastructures	❖ Infrastructures	❖ People
❖ Secondary	❖ Commerce/People	❖ Commerce/People	❖ Infrastructures/Commerce
❖ Vulnerability	❖ Indiscriminate	❖ Indiscriminate	❖ Weakest Link
Impact:			
❖ Spatial	❖ Regional/Worldwide	❖ Local/Regional	❖ Local
❖ Temporal	❖ Years	❖ Months/Years	❖ Month/Years
❖ Damage	❖ Medium/Large	❖ Medium/Large	❖ Medium/Large

The question remains: Are there differences between natural, accidental and willful disruptions? The answer is an emphatic yes; indeed, these differences point to the earlier stated need for a more adaptive, informed and decision-oriented approach to dealing with willful acts than to reacting to natural and accidental disasters. More specifically, Table 2 considers the different types of disruptions from four perspectives: cause, onset, target, and impact.

While the natural causes are obvious, the accidental and willful causes deserve additional discussion. Human errors (as in the case of not following safety procedures in the Bhopal incident) are clearly the most common reason for accidents, while structural failures could include equipment malfunctions (as in the case of three failed flight control systems on United 232). On the other hand, willful or malevolent acts usually involve the use of a destructive weapon (as in the case of a bomb in Oklahoma City, sarin gas in the Tokyo Subway, and airliners in 9/11). There are, of course, a host of other weapons that can be employed to assist the terrorist in his/her act, ranging from conventional explosives, to physical force, to cyber agents, to electromagnetic interference, to the use of a nuclear (including "dirty bombs" or radiological dispersal devices), biological or chemical weapon of mass destruction (WMD).

In regard to its onset, a natural disaster might take hours or days to form (as in the case of Hurricane Camille); as a result, it is highly predictable (consistent with the laws of nature) and not very adaptable to other than natural forces. An accidental tragedy might take hours to unfold (as in the case of Chernobyl); as a result, it is somewhat predictable and not very adaptable to other than the course it is destined for. On the other hand, a willful act, although most likely pre-planned, is still opportunistic in nature and takes only minutes to execute (as in the case of Oklahoma City); as a result, it is quite unpredictable and equally adaptable as new opportunities or threats unfold. It is this quixotic characteristic that makes a willful act difficult to prepare for, to predict, to prevent, to detect, to respond to, and to recover from. Thus, given that terrorists are informed, intelligent and passionate human beings, they must be checked or countered by more informed, more intelligent and more passionate security personnel, who are able to make better decisions, based on multiple data sources, data fusion and analysis methods, timely information, stochastic decision models and systems engineering techniques.

Assuming that the possible targets of a disruption are people, infrastructures and commerce and given today's level of technology, both natural disasters and accidental tragedies, while indiscriminate in their target, tend to primarily damage infrastructures (as in the case of Camille and United 232, respectively) and secondarily disrupt commerce or injure people. Willful acts, on the other hand, primarily seek out the weakest links and focus on injuring people, both physically and psychologically (as in the case of 9/11) and secondarily damage infrastructures or disrupt commerce. Again, this focus on people and their psyche is what makes willful acts especially heinous and elusive.

Finally, in regard to impact, a natural disaster tends to be more regional or world-wide than local (as in the case of SARS), and its effect could last for years. An accidental tragedy tends to be more local or regional (as in the case of Chernobyl) in impact, and it could last for months or years. Thus far, willful acts have mostly had a local impact (as in the case of 9/11), and their effect have lasted for months or years. Of course, a WMD or internet attack could certainly have a world-wide impact and have a detrimental effect for many years. In terms of mortality, morbidity, physical, environmental and financial damages, all major disruptions would most likely result in medium- or large-scale damages, depending on the spatial and temporal dimensions of the disruption.

3. Stages in a Disruption

The mission and overriding objective of the U. S. Federal Emergency Management Agency (FEMA), which is now a part of the 2002 established Department of Homeland Security (DHS) (Public Law 107-296, 2002), is to help the nation be ready to respond to disasters and disruptions of all kinds through a comprehensive, risk-based emergency preparedness program. FEMA develops and

delivers emergency management and first responder training programs; coordinates and develops plans, resources and national standards for emergency response operations; and develops and coordinates assessments and exercises. Traditionally, FEMA's comprehensive emergency management system is composed of four stages (Wallace and De Balogh, 1985): preparedness, mitigation, emergency response and recovery. From a decision perspective, it is helpful to consider an expanded, six-stage process: preparation (corresponding to preparedness), prediction, prevention (corresponding to mitigation), detection, response (corresponding to emergency response), and recovery (corresponding to recovery). The additional prediction stage is necessary because it is beyond general preparation and helps focus and initiate prevention tactics; it requires a set of methodologies and/or technologies that is statistical in nature and risk-based in approach. The additional detection stage is also necessary; it follows prediction and precedes response and is very much dependent on data obtained from multiple data sources or sensors and the careful fusion and analysis of that data.

Table 3 identifies the six stages of a disruption's life cycle in terms of related decisions that must be considered at each stage. Alternatively, Table 4 identifies the six stages of a disruption's life cycle in terms of the 36 target capabilities that the Office of State and Local Government Coordination and Preparedness has identified (DHS, 2005), as a result of their consideration of the 15 afore-mentioned plausible disruption scenarios. The target capabilities have each been allocated to their primary disruption stage based on the level of decision making that it is focused on. Thus, the detection and response stages of a disruption are focused on operational decisions or capabilities; the prediction and prevention stages are focused on tactical capabilities; and the preparation and recovery stages are focused on strategic capabilities. The discussions below highlight some of the critical issues associated with each stage.

3.1 Preparation

In preparing for a major urban disaster, it is critical to learn from past incidents. Careful analysis of past natural disasters, accidental tragedies and willful acts highlight points of vulnerability, decisions that should not have been made, decisions that should have been made, etc. For example, the actions of the first responders are especially pertinent. Their access to protective gear (e.g., masks and air purifying respirators), water for fire suppression, communications for coordination and control, and power for a variety of needs, including lighting and debris removal, must be examined. The roles of fire trucks, ambulances, emergency medical, trucks, buses, and subways in transporting public safety personnel and needed materiel in to the incident site and civilians and the injured out of the site must be choreographed to determine the weaknesses and strengths of the first response process. Most importantly, were the available data from sensing and monitoring devices, both mobile and in situ, regarding the

Table 3 Life Cycle of a Disruption: Stages and Related Decisions

Stages	Related Decisions
Preparation	❖ How and where do terrorist groups form and recruit?
	❖ How are targets picked and what motivates a willful act?
	❖ How to convert potential terrorists away from terrorism?
	❖ How to prepare for disruption without degrading quality of life and civil liberties?
	❖ How to integrate the help of industry and other private organizations?
	❖ What type of resources (e.g., protective gear) are available and at what locations?
	❖ What integrated emergency command center needs to be established?
	❖ How to coordinate and standardize data, medical records, information systems, and communications?
	❖ Is the preparation appropriate for both security and safety?
	❖ How to effectively assess preparedness?
Prediction	❖ What precursor signals can be associated with natural, accidental and willful incidents?
	❖ What is the nature (e.g., self-assembled, self-replicated) and scope of such attacks?
	❖ What facilities, assets and resources are most vulnerable to attack?
	❖ In addition to direct threats, what are possible indirect or secondary threats (e.g., Zoonotic diseases, hurricane-related fresh water flooding)?
	❖ How best to pre-position resources for the most likely and most risky disruptions?
	❖ How to communicate accuracy of prediction?
	❖ How to provide education and simulated training for decision makers and responders?
Prevention	❖ What identification (e.g., biometric) technologies can be reliably employed to prevent unlawful entry?
	❖ How to prevent attacks, reduce vulnerability, minimize damage, and enhance recovery?
	❖ How to develop contingency plans or backup systems to mitigate interdependency problems?
	❖ How to warn the public (e.g., color-coded alerts, terrorist threat index)?
	❖ How and when to mitigate (e.g., evacuate) before the disruption?
	❖ How to mitigate problems of communications, traffic gridlock, and inter-jurisdictional issues?
	❖ How to prevent problems associated with the roles and responsibilities of all involved?
	❖ Are the prevention strategies sustainable and are they commensurate with the risk level?

Stages	Related Decisions
Detection	❖ What sensors can be employed to detect a disruption? ❖ How to fuse and abstract valid and useful information from multiple data sources? ❖ What response preparation should be effected (e.g., level of emergency)? ❖ How to validly identify nature of attack? ❖ What is the target (including people, infrastructures and commerce) and scope (including time, space, and weapon used) of the attack? ❖ How to mitigate the potential impact of an attack? ❖ How to strengthen the public's resilience to the disruption?
Response	❖ Where should an emergency staging and medical triaging center be established? ❖ How to logistically inventory and disburse available resources, requested resources, and donated goods? ❖ How to coordinate and secure communications by computer, cellular, radio, and telephone lines? ❖ How to reposition resources for another attack or response to other incidents? ❖ How to coordinate and integrate workers and volunteers? ❖ How to coordinate within and between response levels (i.e., local, regional, state, and federal)? ❖ How to communicate with the public, including dealing with the media?
Recovery	❖ Which targets remain at risk and must be taken out of harms way? ❖ What can be done to recover from the resultant damages? ❖ How to store, protect, retrieve and recover critical data? ❖ What state, federal and commercial aid can be obtained to fund the recovery? ❖ What recovery goals, measures and assessment procedures have been established? ❖ What projects, tasks, budget and schedule are necessary for the recovery? ❖ What can be put in place to forestall or prepare for another disruption?

Table 4 Stages of a Disruption: Primary Foci of Target Capabilities

Stages (Decision Level)	Primary Foci of Target Capabilities
Preparation (Strategic)	1. All Hazards Planning: plans, policies, procedures, guidelines, mutual aid agreements, etc.

Stages (Decision Level)	Primary Foci of Target Capabilities
	2. Animal Health Emergency Support: foreign animal disease plans, protocols, epidemiology, etc. 3. Critical Resource Logistics & Distribution: stockpiles, maintenance services, security plans, etc. 4. Environmental Health & Vector Control: health protection & organism control plans, procedures, etc. 5. Firefighting Operations/Support: plans, policies & procedures for major/simultaneous incidents, etc. 6. Food & Agriculture Safety & Security: tracking systems, international coordination, sampling, etc. 7. Hazardous Materials (HAZMAT): plans & procedures for HAZMAT mitigation, restoration, etc. 8. Isolation & Quarantine: statutes, regulations, plans, policies, procedures, agreements, arrangements, etc. 9. Mass Care (Sheltering, Feeding, & Related Services): plans, facilities, logistics, agreements, etc. 10. Mass Prophylaxis & Vaccination: plans, dispensing methods & locations, providers, volunteers, etc.
Prediction (Tactical)	11. Emergency Public Education: media-specific materials, programs, procedures, drills, etc. 12. Hazard & Vulnerability Analysis: warning systems, response support guidelines, coordination, etc. 13. Information Collection & Threat Recognition: identification, collection, processing, guidance, etc.
Prevention (Tactical)	14. Criminal Investigation & Intervention: terrorism-related investigative processes, procedures, etc. 15. Critical Infrastructure Protection & Risk Management: identification plan, protective measures, etc. 16. Emergency Evacuation: general & special needs plans, policies, procedures, transportation, etc. 17. Emergency Public Information: accurate, consistent, timely, warnings, media coordination, etc. 18. Medical Supplies Management & Distribution: procurement, rotation, maintenance, location, etc. 19. Urban Search & Rescue: plans, policies, procedures, agreements, mutual aid agreements, training, etc.

Stages (Decision Level)	Primary Foci of Target Capabilities
Detection (Operational)	20. Explosive Device Detection & Response Operations: explosive ordnance disposal teams, etc. 21. Information Sharing & Collaboration: standardized plans, protocols, procedures, exercises, etc. 22. Intelligence Fusion & Analysis: operational policies, protocols, procedures, assessments, etc.
Response (Operational)	23. Emergency Operations Center: command structure, coordination, communications, etc. 24. Emergency Response Communications: security, redundancy, fault-tolerance, non-intrusiveness, etc. 25. Engineering: damage assessments, mitigation activities, technical assistance, etc. 26. Fatality Management: identify, collect, transport & store human remains, belongings, properties, etc. 27. Medical Surge: triage, treatment, transportation, beds, supplies, pharmaceuticals, laboratories, etc. 28. On-Site Incident Management: per National Incident Management System/National Response Plan, etc. 29. Pre-Hospital Triage & Treatment: center located, professionals activated, patients stabilized, etc. 30. Public Health Epidemiological Investigation & Laboratory Testing: plans, protocols, coordination, etc. 31. Public Safety & Security Response: debris removal, ingress, egress, traffic control, logistics, etc. 32. Volunteer Management & Donations: volunteer centers, donation staging areas, logistics, etc. 33. Water Search & Rescue: plans, policies, procedures, distress calls monitoring, rescue operations, etc. 34. Worker Health & Safety: plans, guidelines, standards, equipment, follow-up psychological support, etc.
Recovery (Strategic)	35. Economic & Community Recovery: size, scope, aid, coordination, prioritization, etc. 36. Restoration of Lifelines: damage assessments, contingent contracts, supplemental services, etc.

physical environment, air, water, structures, and resources presented in a meaningful manner for timely and judicious decision making by individual responders or a group of decision makers?

In regard to willful terrorist acts, one has to prepare for the unforeseen or unexpected, including the possibility that an act could include several related actions at different locations. As examples, the 9/11 tragedy included four airline crashes within a regional area and the Sarin attack included five affected subway lines leading to Tokyo center. Obviously, these terrorist acts could have been even more fatal if all response resources were committed to the first occurring action; indeed, this could have occurred if hours, not minutes, were to have separated each action. In short, one must be prepared for the worst possible scenario without bankrupting either our economy or our quality of life.

Perhaps the weakest link in the preparation against a terrorist act is the unwillingness of intelligence organizations to communicate or share crucial information. In fact, as discussed later, many of the activities being undertaken by the U. S. Department of Homeland Security focus on ameliorating or mitigating this problem. Actually, this communication and information sharing problem pervades and adversely impacts every disruption stage, from preparation to recovery. For example, the Federal Bureau of Investigations' recent $170 million effort to establish a Virtual Case File of interview reports throughout the Bureau has been somewhat of a failure, partially due to the fact that agents are reluctant to share their notes for fear of security breaches. Moreover, it can take several days before the available reports are scanned into the central computer, resulting in a potentially dangerous time lag for a fast-moving terrorist initiative.

It is critical for an urban center to prepare not just for urban security but also for urban safety. This dual purpose reflects reality, in that most, if not all, of the public safety resources are able to also secure the homeland; indeed, natural disasters and accidental tragedies result in safety concerns, while only willful acts result in security concerns. Moreover, the costs associated with performing security duties can be considered to be a marginal add-on to the long established public safety mandate.

3.2 Prediction

In many regards, prediction parallels the preparation stage of a disruption. For a past type of disruption, preparation should already be made and prediction can then be employed to determine the likelihood that it might happen again. For a new type of disruption, prediction is necessary to first ascertain the potential nature of the disruption in all its dimensionalities, together with a level of confidence or accuracy regarding the prediction; this would then provide the reason for and the scope of a preparation plan. Thus, prediction details the likelihood, as well as the who, when, what and where, of a disruption. Based on this input, especially the likelihood statistic, appropriate preparation steps can be taken. Moreover, prediction should not only be about the first order impact of a disruption but also about higher-order impacts. In fact, secondary impacts are sometimes more devastating than the initial disaster; thus,

hurricane-caused fresh water flooding of inland rivers and lakes may be more problematic than the initial coastal damages.

Likelihood is a difficult concept to convey to the general public. At present, the U. S. employs an alert system based on five colors ranging from green, the least dangerous, to red, or high alert. The color-coded scheme seeks to capture the likelihood of a terrorist threat and the consequent level of alert or mobilization required. The scheme is too aggregated and is applicable to the entire nation at any point in time. Perhaps a more refined and understandable scheme might be in terms of a terrorist threat index (TTI), much like the Dow Jones Index for stocks and the Consumer Price Index for inflation. TTI could range from, say, 0 to 100, with 100 corresponding to the highest level of alert. Additionally, a gradation of index values should be allowed; thus, for the 9/11 example, the NYC Wall Street area would have had TTI values in the 90s, areas in New Jersey would have had values in the 80s, and upstate New York would have had values in the 70s. Of course, an appropriate decision model must be developed to make the TTI operational; it would be based on a number of contributory factors or variables.

In addition to statistical methods, there are a number of forensic approaches to determining the likelihood of an event. For example, many natural disasters and accidental tragedies are a result of a series of events that signal an impending catastrophe. Recognizing, understanding and appropriately reacting to such events – or precursors – might very well help forestall, if not mitigate, the catastrophe. Willful acts may also register such precursors; for example, increased cellular traffic used to signal an impending terrorist act until the terrorists became more cautious, having realized that the traffic was being monitored.

3.3 Prevention

A critical preventative measure is the use of identification technologies to prevent unlawful entry. For the most part, passwords, identification cards, tokens, keys and codes have been employed. Biometric – including, as examples, fingerprinting, iris scans, voice authentication and face recognition – systems are usually employed where security is critical; they are used for both verification (i.e., one-to-one matching) and identification (i.e., one-to-many matching). To minimize potential errors that may occur, multiple systems are being deployed; for example, foreign visitors to the U. S. must now provide prints of both index fingers and a picture of their face at the port of entry. Another approach suggested by Burnes et al. (2003) is an integrated system whereby, say, the wavelet transforms of both the fingerprints and the facial image are judiciously combined in the wavelet domain and then used for both verification and identification purposes. Although such an integrated or hybrid biometric system might add an extra layer of security, its effect on error rates must still be determined.

The best preventative action in the face of a major disruption and assuming ample warning time is, of course, evacuation. However, cost, inconvenience and believability must all be taken into consideration before an evacuation is ordered. Recently, in August 2004, about a million people were evacuated from an area

south of Tampa, Florida, where Hurricane Charlie, a category 4 storm, was first predicted to come ashore; the evacuation turned out to be a false alarm for many of the evacuated areas. When it was later predicted that the hurricane would come on shore north of Tampa, residents there were reluctant to evacuate, resulting in more damage than necessary if the second set of evacuation warnings were heeded.

Interestingly, in regard to commerce, information technology and supply chain efficiencies have squeezed out many redundancies or inventories; just-in-time everything has been the mantra that has resulted in even greater interdependencies and productivity. Now, however, in order to prevent an adverse impact on the supply chains in the face of a major disruption, there is a need to enhance the reliability of these chains by building in more inventories (i.e., backup systems) and decreasing the interdependencies, resulting in a possible decrease in productivity. Clearly, there is a need to trade off between security and productivity; between just-in-time and just-in-case approaches.

It is critical that whatever prevention tactics or strategies are implemented, are sustainable in the long run. Otherwise, the ever adaptable terrorist will observe a weak link or vulnerability and take appropriate advantage of it. Scaling back on a strategy is more desirable than abandoning it altogether, especially if a statistical approach is taken. Thus, if examining every container at a port of entry is prohibitively costly, then a sampling rate of, say, x percent can be used, with the value of x being commensurate with the assessed risk level.

3.4 Detection

With advances in technology (e.g., micro-electro-mechanical systems, sensor motes, sensor networks, wireless communications, radio frequency identification tags, pervasive computing, and robotics), new devices can be developed to acquire data that may result in the, hopefully early, detection of a natural, accidental or willful incident. Of course, data are just that – data. As discussed in the next section on decision informatics, it takes a careful fusion and analysis of the various data streams to obtain information concerning whether an incident is indeed being detected. Additionally, it is critical that such devices are not compromised. For example, it has been shown that the passive digital signature transponders employed in a number of radio frequency identification (RFID) devices – including vehicle immobilizer keys and SpeedPass-type payment systems – can be successfully attacked with cryptanalytic techniques.

Detection is a critical stage in the life-cycle of a disruption. An alert should be issued if there is ample evidence that an impending disruption may occur. With adequate prior preparation, such an alert should not cause panic but instead begin to mobilize the response resources and, if appropriate, initiate the prevention or mitigation action of evacuation. In fact, if a potential disruption is detected early enough and preventative counter measures can be effectively deployed, then there may not be a need to go to a full-blown response stage. Consequently, more attention should be focused on detection; it could certainly lessen the impact of a disruption and

mitigate, if not obviate, the need for a response.

3.5 Response

How prepared are urban centers to responding to terrorism in the post 9/11 era? The Rand Corporation (Davis et al., 2004) undertook a 2002 survey and found that law enforcement agencies which perceived the risk of a terrorist attack to be higher for their jurisdiction were more likely to undertake steps to improve their corresponding response preparedness. It also found that law enforcement considers the most likely threats to be chemical, biological, or conventional-explosives attacks. Indeed, following 9/11, large cities, especially New York City (NYC), are becoming better prepared, if not coordinated. The lessons learned from the August 14, 2003, northeast power outage also helped the NYC Office of Emergency Management (OEM) develop and adopt a Citywide Incident Management System (CIMS), a formal management structure designed to better organize the City's response to future emergencies. With a unified command matrix and a common understanding of terminologies, roles and responsibilities, the CIMS parallels DHS' National Incident Management System (NIMS) (DHS, 2004(b)).

An important aspect of response concerns how the various data inputs are fused, analyzed and appropriately modeled and presented to the decision makers in a timely manner at both the scene and the command and control centers. The presentation format must facilitate cognition and should not be underestimated, whether it be displayed on a computer or personal data assistant, or visualized on a map, or verbalized in a conversation. Unfortunately, urban centers are, for the most part, ill prepared in this regard. Although, for example, NYC's OEM has a Emergency Operations Center (EOC) where all city agencies plus some state and federal agencies are represented during a crisis situation, periodic situation reports take over an hour to compile from different agency inputs using the E-Team software. These reports – including input from NYC's Citywide Assets and Logistics Management System (CALMS) – are to provide decision support (to the OEM Commissioner and the Mayor) and logistics support (to the field personnel requiring resources). Unfortunately, the reports reflect a minimum amount of data fusion and analysis and cannot be produced in real-time.

Another important aspect of response concerns the immediate establishment of a moveable emergency staging and medical triaging center at or near the disruption site; the center should, of course, be staffed by pre-trained experts. Yet another critical response issue is the repositioning of the unencumbered resources for another attack or in response to other incidents. Media management is likewise critical to the response function, especially since it is the communication link to the citizenry-at-large. There is obviously a fine line between timely sharing of information and delaying that sharing in order to ascertain its accuracy. While unnecessarily panicking the citizenry is not helpful, withholding information, even temporarily, that might affect the citizens' security and safety is also inappropriate, if not

illegal. Simulated training in this difficult area is clearly required.

3.6 Recovery

Depending on the nature of the disruption, alternate recovery steps can be taken. For example, damage to, say, the Wall Street financial system would require careful reconstruction or recovery of the vital data, most of which should have been backed up on an off site server. Rebuilding of a physical structure would, of course, require more intense planning and execution.

No matter what the disruption is, the first step is to stabilize the situation and then to ascertain the damages. The next necessary step is to determine the resources – including state and federal aid, as well as commercial insurance payouts – required to adequately, if not fully, recover from the disruption. The amount of resources is, of course, also subject to the stated rules and regulations governing their availability. Again, having access to knowledgeable and pre-trained experts in this area would minimize victim frustrations and facilitate the recovery effort, which could take months, if not years, to carry out.

4. Decision Informatics

In critically reviewing the disruption characteristics in Table 2 and related decisions identified in Table 3 and 4, it is obvious that real-time, information-based decision making is needed for addressing major disruptions, especially in regard to terrorist acts that are quite adaptive in reality. Alternately, what is needed is, as depicted in Figure 1, a decision informatics paradigm. That is, the nature of the required real-time decision (in connection with each of the six stages of a disruption) determines, where appropriate and from a systems engineering perspective, the data to be collected (possibly, from multiple, non-homogeneous sources) and the real-time fusion and analysis to be undertaken to obtain the needed information for input to the modeling effort which, in turn, provides the knowledge to support the required decision in

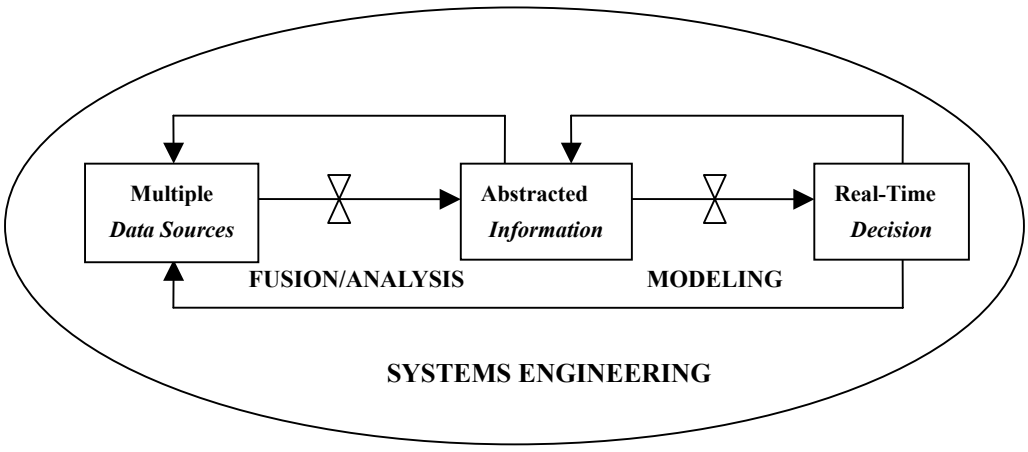

Figure 1 Decision Informatics Paradigm

a timely manner. The feedback loops in Figure 1 are within the context of systems engineering; they serve to refine the analysis and modeling steps.

Thus, decision informatics concerns three related issues (i.e., decisions, data and information) and is underpinned by three multi-disciplines (i.e., data fusion and analysis, decision modeling, and systems engineering). In abbreviated form, there are six steps in the decision informatics process: decisions, data, analysis, information, models, and systems. These six steps are summarized in Table 5. Before highlighting below some of the concerns at each step, it should be noted that decision informatics is, as a framework, generic and applicable to most, if not all, decision problems. Furthermore, since any data analysis or modeling effort should only be undertaken for some purpose or decision, all analyses and modeling activities can be viewed within the decision informatics framework. In short, decision informatics represents a decision-driven, information-based, adaptive, real-time, human-centered, integrated and computationally-intensive approach to intelligent decision making by humans or software agents. Consequently, it can be very appropriately employed to address decisions at the preparation, prediction, prevention, detection, response, and recovery stages of an urban disruption.

4.1 Decisions

As noted earlier, effective urban emergency management is not only about making the right decisions; it is also about making timely decisions. For example, moving analysts closer to the decision maker would be most helpful in a real-time environment where management failures and communications breakdowns are more prevalent given the heightened pressures of time, urgency and criticality. This would be especially pertinent at the operational level (which, as indicated earlier, includes the detection and response stages of a disruption) where decisions must be made in real-time.

On the other hand, at the tactical level (which includes the prediction and prevention stages of a disruption), decisions must be made in terms of days, if not hours; and at the strategic level (which includes the preparation and recovery stages of a disruption), decisions must be made in terms of months, if not weeks. No matter at what level a decision is made, it is critical to note that steady state analysis or models are of limited use in addressing the emergency management of urban disruptions.

Although decision support models focus on helping one or more decision makers to make the best informed decisions, it should be noted that most decisions are made in a collective, if not collaborative, manner among a group of decision makers. This is especially true in the public sector where elected officials depend on their appointees to help them make the decisions, subject to a number of other constraints – including political, budgetary and social equity issues – that may not be implicitly considered in the models. Clearly, in terms of a major urban disruption, collective or group decision making occurs at every stage of a disruption's life cycle, from preparation to recovery. The National Science Foundation's recent focus on advancing collaborative systems is helpful in this regard.

Table 5 Decision Informatics Steps

Steps	Considerations
Decisions	
❖ *Disruptions*	❖ Natural, Accidental, Willful
❖ *Levels*	❖ Operational, Tactical, Strategic
❖ *Targets*	❖ People, Infrastructures and Commerce
Data	
❖ *Attributes*	❖ Measurability, Availability, Consistency, Validity, Reliability, Stability, Accuracy, Independence, Robustness, Completeness
❖ *Sources*	❖ Sensors Intelligence (SENSINT), Signals Intelligence (SIGINT), Imagery Intelligence (IMINT), Human Intelligence (HUMINT)
❖ *Issues*	❖ Standards, Compatibility, Interoperability, Scale
Analysis	
❖ *Types*	❖ Data Fusion, Data Analysis, Data Mining, Data Interpolation, Evolutionary Algorithms, Strengths, Weaknesses, Opportunities, Threats
❖ *Disciplines*	❖ Decision Analysis (Statistics, Risk Analysis, Operations Research, Economics), Science (Information, Cognition, Psychology, Sociology, Behavior, Organization, Computer, Agriculture, Livestock, Food, Ocean, Atmosphere), Engineering (Telecommunications, Human Factors, Biomedical, Chemical, Nuclear), Other (Religion, Terrorism, Culture)
Information	
❖ *Attributes*	❖ Same As Data Attributes
❖ *Sources*	❖ Same As Data Sources
❖ *Types*	❖ Threats, Vulnerabilities, Risks, Damages (Mortality, Morbidity, Physical, Environmental, Financial)
❖ *Issues*	❖ Same As Data Issues
❖ *Characteristics*	❖ Processed Data, Derivations, Groupings, Patterns
Models	
❖ *Types*	❖ Descriptive (System Dynamics, Simulation), Prescriptive (Mathematical Programming, Dynamic Programming), Adaptive (Evolutionary Models, Bayesian Networks)
❖ *Disciplines*	❖ Same as Analysis Disciplines
Systems	
❖ *Attributes*	❖ Intra/Interdependent, Natural/Human-Made, Physical/Conceptual, Static/Dynamic, Closed/Open
❖ *Resources*	❖ Law Enforcement, Firefighting, Public Works, Public Health, Emergency Medical, Private, Financial
❖ *Networks*	❖ Private (Organizations, Institutions), Public (Local, Regional, State, Federal), Cyber
❖ *Issues*	❖ Privacy, Civil Liberties, Quality of Life

4.2 Data

Sensors acquire data; they could be in the form of humans, robotic networks, aerial images, electronic signals, and other measures and signatures. In regard to tsunamis, for example, seismographs, deep ocean detection devices with buoy transmitters, and/or tide gauges can all sense a potential tsunami. Other sensors are being developed to detect weapons of mass destruction. One such effort is being undertaken by CombiMatrix; under a $10 million funding, a computer chip is being developed that can sense up to 20 different threats, from biological agents like anthrax to deadly chemicals and radiation. However, as noted earlier, data are useless unless access to and analysis of the data are in real-time and, moreover, the findings are also transmitted in a timely manner to a public which should have been prepared to react appropriately and not in a panic. There were clearly gaps in the preparation, detection, response and recovery stages of the 2004 South Asia Tsunami.

More recently, data warehouses are proliferating and data mining techniques are gaining in popularity. No matter how large a data warehouse and how sophisticated a data mining technique, problems can, of course, occur if the data do not possess the desirable attributes of measurability, availability, consistency, validity, reliability, stability, accuracy, independence, robustness and completeness. Indeed, 9/11 might have been thwarted if a more robust and system-oriented passenger screening system were in place instead of the 1998 initiated CAPPS program (which employed a computer-based formula to identify potential terrorists based on a number of variables), a program that had already experienced a drastic cutback, and, moreover, had not been uniformly used by the airlines. Hopefully, most of these deficiencies have been corrected in the current Transportation Security Administration's CAPPS II system.

To be more specific and as illustrated in Table 5, the definition and collection of data must be motivated by the decisions that must be made based upon the information that is obtained from the processing (i.e., fusion and analysis) of the data. More importantly and from an urban emergency management perspective, a collaborative, decision-driven data base management system must be developed that can electronically access locally-generated data and provide appropriate information (through data fusion and analysis algorithms and decision support models) for real-time, distributed decision making. It should be noted that currently available collaborative software systems (e.g., E-Team) are stand-alones that are neither directly interfaced with critical data sources nor supported by appropriate decision-oriented algorithms and models.

4.3 Analysis

Data fusion and analysis methods include probability, statistics, quality, reliability, fuzzy logic, multivariable testing, pattern analysis, etc. as well as the mining, visualization and management of data, information and knowledge. However, the fusion and analysis of data to yield valid information or intelligence is not only about the application of these methods; it is also about specialized analysts who have, as examples, the linguistic

skills to translate important data, the ability to develop software agents to troll the Web (especially the forthcoming Semantic Web with its definitional tags) for valuable information, and the cultural or religious background to interpret the data. In short, it takes a terrorist mind to help develop appropriate data fusion and analysis techniques and then to recognize the relevant information gleaned from the analysis, as well as to help make informed decisions to prepare for, to predict, to prevent, to detect, to respond to, and to recover from a potential terrorist act.

The National Visual Analytics Center, established by DHS in 2004 under the auspices of the Pacific Northwest National Laboratory, is developing tools that are capable of creating images from complex multidimensional data which, in turn, could enable analysts to effectively fuse and analyze data streams containing structured and unstructured text documents, measurements, images and video data. Obviously, such tools would be invaluable in the prevention and detection of terrorist acts. The fusion and analysis of qualitative and quantitative data take on an extra dimension of difficulty when both steps have to be undertaken in real-time (Hu and Tien, 2004).

In business, a strengths, weaknesses, opportunities and threats (SWOT) analysis is undertaken to obtain valid information that can be used to make informed business strategies. Likewise, effective security strategies can be identified by using a similar information-based approach. Thus, S-O strategies could focus on prevention opportunities that are a good fit to the law enforcement strengths of, say, a city; W-O strategies could focus on overcoming preparation weaknesses by pursuing cooperative regional opportunities; S-T strategies could focus on ways that the city can use its firefighting strengths to reduce vulnerabilities to another 9/11 threat; and W-T strategies could focus on a security and reliability plan to prevent the city's interdependent infrastructure weaknesses from making it highly susceptible to external terrorist threats.

4.4 Information

As noted in Table 5, information has the same sets of attributes, sources, and issues as data; however, information is processed data and could be in terms of derivations, groupings or patterns. In general, information technology has transformed large-scale information – really data – systems from being the "glue" that holds the various units of an organization together to being the strategic asset that provides the organization with its competitive advantage. However, as alluded to earlier, while information technology can transform a data poor situation into a data rich environment, the fact remains that the data need to be effectively and efficiently fused and analyzed in order to provide appropriate information for decision making. Thus, in order to overcome the somewhat embarrassing data rich, information poor (DRIP) problem that Tien (2003) forewarned, it is critical to develop more sophisticated data fusers and data analyzers that could yield the information or knowledge for making smart choices. In essence, information technology is a necessary, but not sufficient, condition for robust and

timely decision making; the sufficient condition is one based on decision informatics.

Data must be processed to yield timely information on threats, vulnerabilities to these threats, and the possible resultant risks or damages, including mortality, morbidity, physical, environmental, and financial consequences. The results of any analysis must support the cognitive process of mental visualization, capable of creating images from complex multidimensional data, including structured and unstructured text documents, measurements, images and video. Moreover, creating and communicating a mental image common to a team of emergency responders facilitates collaboration and leads to more effective decision making at all levels, from operational to strategic.

4.5 Models

As noted above, at the operational level, there is a need for real-time decision support models. In such a situation, it is not just about speeding up the models and their solution algorithms; indeed, steady state models become irrelevant in a real-time environment. In essence, it concerns reasoning under both uncertainty and time constraints. Santos and his colleagues have contributed extensively to this area: they (Santos, 1996) have employed linear potential functions to approximate solutions to decision problems cast as Bayesian networks; they (Santos and Young, 1999) have formulated uncertain temporal reasoning without the use of Markov models and yet have been able to elegantly cope with the resultant combinatorial overhead; and they (Santos et al., 2003) have developed a seminal way of incrementally updating Bayesian knowledge bases. These efforts are closely aligned with evolutionary models, also known as genetic algorithms that work in a manner similar to biological evolution or natural selection. The algorithms are based on a seminal paper by Holland (1962) that posited a logical theory for adaptive systems. However, these algorithms did not become a viable tool until computers became powerful enough to start with equations that offer potential solutions, then mutate them repeatedly in an evolutionary manner until a solution emerges that best fit the observed data. Today, evolutionary algorithms have been employed to coordinate airport operations, to develop assembly line schedules, to enhance autonomous operations in unmanned aircrafts, and to determine sniper locations while on patrol in Iraq. The question remains: could such adaptive models help urban centers detect and respond to a major disruption? Certainly, adaptive models are better suited to dealing with changing situations and threats than the more traditional descriptive or prescriptive models. Nevertheless, evolutionary algorithms must be further developed and become more dynamic in their adaptiveness in order to capture the equally adaptive or elusive behavior of terrorists who are experts at modifying their actions and avoiding detection.

At a more tactical level and as Larson (2004, 2005) details, there is a range of decision models for emergency response planning. Indeed, response to an emergency is about allocating or reallocating resources, which is the essence of operations research – a science that helped the U. S. minimize

shipping losses during World War II, brought efficiencies in production, and developed optimal scheduling of police and firefighters. Actually, much of the urban emergency response modeling came out of the efforts of the New York City-RAND Institute (NYCRI), a 1968-1975 partnership between the RAND Corporation and New York City (Green and Kolesar, 2004). For example, the NYCRI fire allocation model, developed almost 30 years before 9/11, was invaluable in helping New York City deploy and redeploy their fire resources on that fateful day. Another set of critical tactical models includes those that can simulate, as examples, the impact of an airliner hitting a chemical plant, the dispersion of radioactive material following the explosion of a dirty bomb, and the spread of illness due to a contaminated water supply.

At the strategic, policy or preparedness level, there are a number of appropriate models that can support such decisions. As examples, Kaplan et al. (2002) developed a set of complex models to demonstrate that the best prevention strategy to a smallpox attack would be to undertake immediate and widespread vaccination; Wein et al. (2003) similarly advocate for a widespread dispersion of antibiotics following an anthrax attack; and Yu et al. (2003) developed an effective airline recovery algorithm that can be applied following an extended halt in operation, as happened in 9/11. Unfortunately, models, including simulations, dealing with infrastructures and their interdependencies are still relatively immature and must be the focus of additional research and development. Such "system of systems" models will, undoubtedly be very complex and will require a multidisciplinary approach.

4.6 Systems

Systems engineering is about integrating products, processes and operations from a holistic perspective, especially human-centered systems that are computationally-intensive and intelligence-oriented. It can be considered a multidiscipline that addresses a system from a life-cycle and cybernetic (i.e., feedback and control) perspective. A critical aspect of systems engineering is system performance; it provides an essential framework for assessing the decisions made – in terms of such issues as satisfaction, convenience, privacy, security, equity, quality, productivity, safety and reliability. Given the interdependencies of urban infrastructures, it is especially crucial to address an urban disruption from a systems perspective. Indeed, even within an infrastructure or system, one needs to address it from a holistic framework, especially in regard to weak links in the system. For example, although the airline industry has significantly increased the security screening of passengers and luggage at major airports, it may still be possible for a terrorist to enter the system through a regional airport where screening is not as thorough. Nevertheless, undertaking systems engineering within a real-time environment will require – as with decisions, data, analysis, information and modeling – additional research and development.

A fundamental underpinning of a democratic system is personal privacy. It is obvious that every time one uses a credit card

or an electronic device to enter a building or to get by a toll booth, one is giving up personal data, some of which are being compiled by a number of intelligence-oriented companies (e.g., Acxiom, ChoicePoint and Seisint). These companies, initially established to help market products, are apparently filling the void left by the Pentagon's Total Information Awareness program, which Congress cancelled in 2003 after it became a lightning rod for privacy advocates alarmed about unchecked government surveillance. O'Harrow (2005) takes a look at this trend and warns that such surveillance programs reflect a shadowy new alliance between private sector firms and government agencies, one that is unaccountable and allows for no due process and redress when one is being unfairly harmed or compromised.

5. Homeland Security

Following the 9/11 attack on the U. S. homeland in 2001, the U. S. Homeland Security Act of 2002 (Public Law 107-296, 2002) was immediately passed; it established the Department of Homeland Security (DHS) with a mission to "a) prevent terrorist attacks within the United States; b) reduce the vulnerability of the United States to terrorism; and c) minimize the damage, and assist in the recovery, from terrorist attacks that do occur within the United States." Additionally, a number of high level reports have been published on how to make the homeland more secure from future acts of terrorism. The U. S. National Academies formed a Committee on Science and Technology for Countering Terrorism (2003); it strongly urged, among several other important recommendations, a risk or decision based approach to measuring and countering terrorism, and it also helped to define the Directorate of Science and Technology that is now a part of DHS. More recently, the National Commission on Terrorist Attacks Upon the United States (2004) recommended the establishment of a National Counterterrorism Center – with a National Intelligence Director – to unify all counterterrorism intelligence and operations across the foreign-domestic divide in one organization.

The strategic goals of DHS (2004(a)) include i) awareness (i.e., identifying and understanding threats, assessing vulnerabilities, determining potential impacts and disseminating timely information to security partners and the public); ii) prevention (i.e., detecting, deterring and mitigating threats); iii) protection (i.e., safeguarding the people and their freedoms, critical infrastructures, property, and the economy from acts of terrorism, natural disasters, or other emergencies); iv) response (i.e., leading, managing and coordinating the national response to acts of terrorism, natural disasters, or other emergencies); v) recovery (i.e., leading national, state, local and private sector efforts to restore services and rebuild communities after acts of terrorism, natural disasters, or other emergencies); vi) service (i.e., serving the public effectively by facilitating lawful trade, travel and immigration); and vii) organizational excellence (i.e., creating a culture that promotes a common identity, innovation, mutual respect, accountability and teamwork to achieve efficiencies, effectiveness,

and operational synergies). Not surprisingly, the first five of the above identified seven DHS goals cover the earlier detailed six stages of a disruption.

As stated in two related Presidential directives (U. S. President, 2003(a,b)), the National Response Plan (DHS, 2004(c)) establishes a comprehensive all-hazards approach to enhance the ability of the nation to manage domestic incidents. The National Response Plan (NRP) incorporates best practices and procedures from incident management disciplines—homeland security, emergency management, law enforcement, firefighting, public works, public health, responder and recovery worker health and safety, emergency medical services, and the private sector—and integrates them into a unified structure. It forms the basis of how the federal government coordinates with state, local, and tribal governments and the private sector during incidents. It establishes protocols to help i) save lives and protect the health and safety of the public, responders, and recovery workers; ii) ensure security of the homeland; iii) prevent an imminent incident, including acts of terrorism, from occurring; iv) protect and restore critical infrastructure and

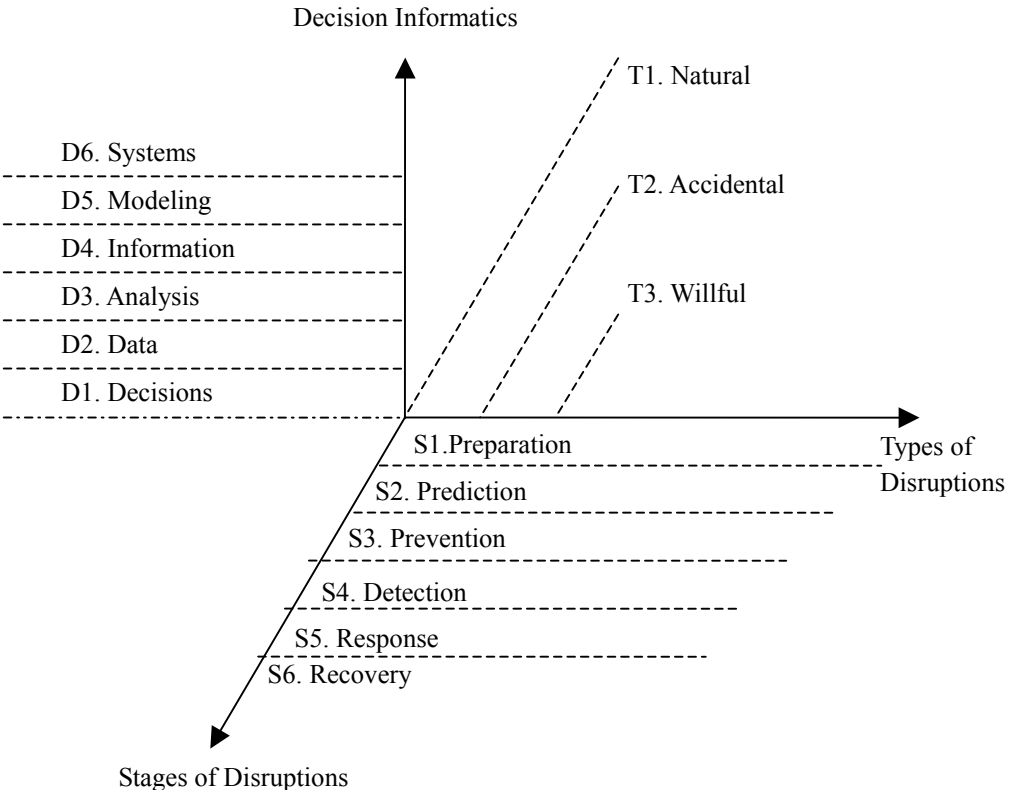

Figure 2 Urban Disruptions: Types, Stages and Decisions

key resources; v) conduct law enforcement investigations to resolve the incident, apprehend the perpetrators, and collect and preserve evidence for prosecution and/or attribution; vi) protect property and mitigate damages and impacts to individuals, communities, and the environment; and vii) facilitate recovery of individuals, families, businesses, governments, and the environment. Further, to enhance the ability of the nation to manage domestic incidents, a single, comprehensive National Incident Management System (NIMS) has been established (DHS, 2004(b)). The NRP is predicated on the NIMS; together, the NRP and the NIMS provide a nationwide template for working together to prevent or respond to threats and incidents regardless of cause, size, or complexity.

The Department of Homeland Security (DHS) is organized into four major directorates: Border and Transportation Security (including sensors, signals, passenger profiling, and prevention tactics), Emergency Preparedness and Response (including preparation, prediction, prevention, detection, response, and recovery), Information Analysis and Infrastructure Protection (including data fusion and analysis, disruption modeling, performance versus cost analysis, vulnerability/risk assessment tools and systems considerations), and Science and Technology (including biometric systems, weapons detection systems, and satellite image systems). DHS actually out sources many of its activities through contracts and grants – to federal laboratories, government agencies, and private organizations. In April 2004, the $130M, 4.5-year Homeland Security Institute was established at Analytic Services, Inc. or ANSER, a systems engineering "think tank" modeled after the RAND Corporation.

Additionally, through the Office of University Programs within the Science and Technology Directorate, DHS is engaging the academic community to create learning and research environments in areas critical to homeland security. DHS is investing in university-based partnerships for two reasons. First, to bring together the nation's best experts and to focus its most talented researchers on a variety of threats that include agricultural, chemical, biological, nuclear, explosive and cyber terrorism as well as the behavioral aspects of terrorism. An equally important reason to engage the academic community is to enhance the nation's knowledge capacity and people resources to deal with natural disasters, accidental tragedies and willful acts through relevant education and training. Labeled Homeland Security Centers of Excellence, it is helpful to consider them within the three dimensional – types, stages and decisions – framework discussed in the previous sections of this paper. As depicted in Figure 2, this framework identifies 3 by 6 by 6 or 108 possible foci for study consideration.

Thus far, four Homeland Security Centers of Excellence have been established, while a fifth one is forthcoming. As summarized in Table 6, the DHS awarded in November 2003 the first Center of Excellence to the University of Southern California, in partnership with the University of Wisconsin at Madison, New York University, North Carolina State University, Carnegie Mellon University, Cornell University, and others. Known as the

Homeland Security Center for Risk and Economic Analysis of Terrorism Events (CREATE), the 3-year, $12 million center is focused on the study of risk analysis as related to the economic consequences of terrorist threats and events.

In April 2004, two related 3-year centers were established. Texas A&M University, in partnership with the University of Texas Medical Branch, University of California at Davis, University of Southern California and University of Maryland, was awarded $18 million to establish a Homeland Security National Center for Foreign threats to animal agriculture, including foot-and-mouth disease, Rift Valley fever, Avian influenza and Brucellosis. The related Homeland Security Center for Food Protection and Defense was awarded to the University of Minnesota and its partners – Michigan State University, University of Wisconsin at Madison, North Dakota State University, Georgia Institute of Technology, Rutgers University, Harvard University, University of Tennessee, Cornell University, Purdue University and North Carolina State University. $15 million was awarded to this Center to address agro-security issues related to post-harvest food protection.

The fourth center, entitled Homeland Security Center of Excellence on Behavioral and Social Research on Terrorism and Counter-Terrorism, was awarded in January 2005 to the University of Maryland and its five major partners – University of Colorado, University of Pennsylvania, Monterey Institute of International Studies, University of South Carolina and the University of California, Los Angeles – and 10 other academic institutions in the U. S. and abroad. This 3-year, $12 million effort is focused on understanding the social and behavioral aspects of terrorism so as to disrupt the formation of terror networks and to minimize the impact of future attacks.

The solicitation for a fifth center, entitled Homeland Security Center for the Study of High Consequence Event Preparedness and Response, has just been released in January 2005; it will also be a 3-year Center, funded at a $15 million level. The Center is to perform research on how to prepare for high consequence events, especially in regard to acts of terrorism and the use of weapons of mass destruction (WMD), as well as on how to enhance the capabilities of first responders and others.

Table 6 also identifies the foci of these five academic centers in regard to the types of disruption, the stages of a disruption, and the decisions associated with a disruption. As expected, willful acts constitute the focus of all five centers, while accidental tragedies constitute the focus of three of the centers, and natural disasters constitute the focus of two of the centers. In regard to the six stages of a disruption, three of the stages – preparation, prediction and prevention – are dealt with by all five centers, response is dealt with by four centers, detection is dealt with by three centers, and recovery is dealt with by two centers. Finally, as also might be expected, all six steps – decisions, data, analysis, information, modeling and systems – in the decision informatics process are necessary in each center's approach to their respective problem foci.

Table 6 Homeland Security Centers of Excellence: Focus on Types, Stages and Decisions

Established (3-Year Funding)	Lead/Primary Partner Universities/Others	Scope	Center Name	Types	Stages	Decisions
November 2003 ($12M)	❖ **U. of Southern California** ❖ U. of Wisconsin, Madison ❖ New York U. ❖ North Carolina State U. ❖ Carnegie Mellon U. ❖ Others: Consultants, Academia	❖ Risk analysis related to economic consequences of terrorist threats and events.	❖ Homeland Security Center for Risk and Economics Analysis of Terrorism Events (CREATE)	❖ Willful	❖ Preparation ❖ Prediction ❖ Prevention ❖ Response	❖ Decisions ❖ Data ❖ Analysis ❖ Information ❖ Modeling ❖ Systems
April 2004 ($18M)	❖ **Texas A&M U**. ❖ U. of Texas/Medical Branch ❖ U. of California, Davis ❖ U. of Southern California ❖ U. of Maryland ❖ Others: Industry, Government, Academia	❖ Potential threats to animal agriculture, including foot-and-mouth disease, Rift Valley fever, Avian Influenza, and Brucellosis.	❖ Homeland Security National Center for Foreign Animal and Zoonotic Disease Defense.	❖ Natural ❖ Accidental ❖ Willful	❖ Preparation ❖ Prediction ❖ Prevention ❖ Detection ❖ Response	❖ Decisions ❖ Data ❖ Analysis ❖ Information ❖ Modeling ❖ Systems
April 2004 ($15M)	❖ **U. of Minnesota** ❖ Michigan State U. ❖ U. of Wisconsin, Madison ❖ North Dakota State U. ❖ Georgia Institute of Technology ❖ Others: Major Food Companies	❖ Agro-security issues related to post-harvest food protection.	❖ Homeland Security Center for Food Protection and Defense	❖ Accidental ❖ Willful	❖ Preparation ❖ Prediction ❖ Prevention ❖ Detection ❖ Response	❖ Decisions ❖ Data ❖ Analysis ❖ Information ❖ Modeling ❖ Systems
January 2005 ($12M)	❖ **U. of Maryland** ❖ U. of California, Los Angeles ❖ U. of Colorado, Boulder ❖ Monterey Institute of International Studies ❖ U. of Pennsylvania ❖ U. of South Carolina, Columbia ❖ Others: Academia	❖ Applying social science to the understanding and prevention of terrorism.	❖ Homeland Security Center of Excellence on Behavioral and Social Research on Terrorism and Counter-Terrorism.	❖ Willful	❖ Preparation ❖ Prediction ❖ Prevention ❖ Recovery	❖ Decisions ❖ Data ❖ Analysis ❖ Information ❖ Modeling ❖ Systems
Forthcoming ($15M)	❖ To be awarded.	❖ Ways to prepare for, respond to, and recover from major disasters	❖ Homeland Security Center for the Study of High Consequence Event Preparedness and Response.	❖ Natural ❖ Accidental ❖ Willful	❖ Preparation ❖ Prediction ❖ Prevention ❖ Detection ❖ Response ❖ Recovery	❖ Decisions ❖ Data ❖ Analysis ❖ Information ❖ Modeling ❖ Systems

6. Concluding Remarks

Securing the homeland from damaging willful acts is a matter of tradeoffs. It is a tradeoff between security and people; in particular, people's privacy, civil liberties and quality of life. It is a tradeoff between security and infrastructures; in particular, infrastructures that are highly interdependent. It is a tradeoff between security and commerce; in particular, commerce that is based on highly efficient and non-redundant processes. In short, it is a tradeoff between security and a free society.

Interestingly, the tools or technologies that underpin a modern society are likewise the weapons that can be used to undermine, if not destroy, society. Biological, chemical and nuclear breakthroughs can also be considered to be weapons of mass destruction; the highly effective Internet provides a medium for cyber viruses, hackers and spammers; and airplanes are employed as missiles against people, infrastructures and commerce.

The decision informatics approach to urban emergency management that is detailed herein can clearly address a number of vulnerabilities, including natural disasters, accidental tragedies and willful acts. Several comments should be made in regard to this approach. First, it is multidisciplinary in nature; obviously, depending on the problem being considered, it requires experts from many disciplines. Second, it is evolutionary in practice; as a problem becomes better understood, the approach could be better refined and made more expeditious. Third, it is systemic in scope; it seeks to consider a problem from different perspectives, in terms of, as examples, efficiency and reliability, public and private goals, and domestic and international concerns.

The purpose of this paper, then, is to augur for the development of decision technologies that can be employed to prepare for a major disruption, if not predict and possibly prevent the disruption. Such technologies should also detect the disruption, identify the responses required to deal with the resultant situation, and then, following the disruption, specify the recovery steps that are necessary to satisfactorily recuperate from the disruption.

References

[1] Beroggi, B.E.G. and W.A. Wallace, "Real-Time decision support for emergency management: an integration of advanced computer and communications technology", *Journal of Contingencies and Crisis Management*, Vol. 3, No. 1, pp18-26, 1995.

[2] Burnes, J. P., W. Chang and J. M. Tien "An intrinsic assessment and comparison of biometric systems through wavelet analysis", *2003 IEEE International Conference on Systems, Man, and Cybernetics*, Washington, DC, 2003.

[3] *Committee on Science and Technology for Countering Terrorism (Co-Chairs: L. M. Branscomb and R. D. Klausner), Making The Nation Safer: The Role of Science and Technology in Countering Terrorism*, Washington, DC: The National Academies Press, National Research Council, 2003.

[4] *Committee on The Role of Information Technology in Responding To Terrorism (Co-Editors: J. L. Hennessy, D.A. Patterson, and H. S. Lin), Information Technology for Counterterrorism*, Washington, DC: The

National Academies Press, National Research Council, 2005.

[5] Davis, L. M., K. J. Riley, G. K. Ridgeway, J. Pace, S. K. Cotton, P. Steinberg, K. Damphousse, and B. L. Smith, *When Terrorism Hits Home: How Prepared Are State and Local Law Enforcement*?, Santa Monica, CA: The Rand Corporation, 2004.

[6] Department of Homeland Security (DHS), *Securing Our Homeland: The DHS Strategic Plan*, Washington, DC: DHS, 2004(a).

[7] Department of Homeland Security (DHS), *National Incident Management System*, Washington, DC: DHS, 2004(b).

[8] Department of Homeland Security (DHS), *National Response Plan*, Washington, DC: DHS, 2004(c).

[9] Department of Homeland Security (DHS), *Target Capabilities List*, Washington, DC: DHS, Office of State and Local Government Coordination and Preparedness, 2005.

[10] Green, L. V. and P. J. Kolesar, "Improving emergency responsiveness with management science", *Management Science*, Vol. 50, pp1001-1014, 2004.

[11] Holland, J. H., "Outline for a logical theory of adaptive systems", *Journal of the Association for Computing Machinery*, Vol. 9, pp297-314, 1962.

[12] Hu, J. and J. M. Tien, "Real-time fusion and analysis of multiple non-homogeneous data streams", *Proceedings of the 2004 National Science Foundation Workshop*, Dallas, Texas, 2004.

[13] Kaplan, E. H., D. L. Craft and L. M. Wein, "Emergency response to a smallpox attack: the case for mass vaccination", *Proceedings of the National Academy of Sciences*, Vol. 99, No. 16, pp10935-10940, 2002.

[14] Larson, R. C., M. D. Metzger, and M. F. Cahn, *Emergency Response for Homeland Security: Lessons Learned and the Need for Analysis*, West Newton, MA: Structured Decisions Corporation, September, 2004.

[15] Larson, R. C., "O. R. models for homeland security", *OR/MS Today*, Vol. 31, No. 6, pp22-29, 2004.

[16] Larson, R. C., "Decision models for emergency response planning", in *Handbook of Homeland Security* (D. Kamien, Editor), New York, NY: McGraw-Hill, 2005.

[17] National commission on terrorist attacks upon the united states, *The 9/11 Commission Report*, Washington, DC: U. S. Government Printing Office, 2004.

[18] O'Harrow, R. Jr., *No Place To Hide*, Washington, DC: Free Press, 2005.

[19] Public law 107-296, as amended, *Homeland Security Act of 2002*, Washington, DC: U. S. Congress, H. R. 5005-8, 2002.

[20] Santos, E., Jr., "On linear potential functions for approximating bayesian computations", *Journal of the Association for Computing Machinery*, Vol. 43, No. 3, pp399-430, 1996.

[21] Santos, E., Jr., and J. D. Young, "Probabilistic temporal networks: a unified framework for reasoning with time and uncertainty", *International Journal of Approximate Reasoning*, Vol. 20, pp263-291, 1999.

[22] Santos, E., Jr., E. Santos, Sr., and S. E. Shimony, "Implicitly preserving semantics during incremental knowledge base

acquisition under uncertainty", *International Journal of Approximate Reasoning*, Vol. 33, pp71-94, 2003.

[23] Talbot, D., "Terror's server", *Technology Review*, pp46-52, February 2005.

[24] Tien, J. M., "Towards a decision informatics paradigm: a real-time, information-based approach to decision making", *IEEE Transactions on Systems, Man, and Cybernetics*, Special Issue, Part C, Vol. 33, No. 1, pp102-113, 2003.

[25] U. S. President, *Presidential Decision Directive NSC-63*, Washington, DC: The White House, May 22, 1998.

[26] U. S. President, *Executive Order on Critical Infrastructure Protection*, Washington, DC: The White House, October 16, 2001.

[27] U. S. President, *Homeland Security Presidential Directive (HSPD) 5*, Washington, DC: The White House, February 28, 2003(a).

[28] U. S. President, *Homeland Security Presidential Directive (HSPD) 8*, Washington, DC: The White House, December 17, 2003(b).

[29] Wallace, W. A. and F. De Balogh, "Decision support systems for disaster management", *Public Administration Review*, Vol. 45, Special Issue: Emergency Management, pp134-146, 1985.

[30] Wein, L. M., D. L. Craft, and E. H. Kaplan, "Emergency attack to an anthrax attack", *Proceedings of the National Academy of Sciences*, Vol. 100, No. 7, pp4347-4351, 2003.

[31] Yu, G., M. Arguello, M. Song, S. McCowan, and A. White, "A new era for crew recovery at continental airlines", *Interfaces*, Vol. 33, No. 1, pp5-22, 2003.

James M. TIEN is the Yamada Corporation Professor at Rensselaer Polytechnic Institute, He is also an Honorary Professor at several Chinese Universities and an elected member of the U. S. National Academy of Engineering. He received the BEE from Rensselaer Polytechnic Institute (1966) and the SM, EE and PhD from the Massachusetts Institute of Technology (1967, 1970, 1972). He has held leadership positions at Bell Telephone Laboratories (1966-69), at the Rand Corporation (1970-73), and at Structured Decisions Corporation (1974-Present). His areas of research interest include the development and application of computer and systems analysis techniques to information and decision systems He has been honored with both teaching and research awards, including being elected Fellow (of IEEE, INFORMS and AAAS) and being a recipient of the IEEE/SMC Joseph G. Wohl Outstanding Career Award, the IEEE/EAB Major Educational Innovation Award, and the IEEE/SMC Norbert Wiener Award.