The National Response Plan and the Problems in the Evaluation and Assessment of the Unconventional Modes of Terrorism

Dr. David V. LeMone
University of Texas at El Paso
P.O. Box 3, 500 West University, El Paso Texas, 79968
USA

Dr. Shawn G. Gibbs
U. T. Houston School of Public Health
1100 North Stanton, Suite 110 C, El Paso, Texas 79902
USA

John W. Winston, Jr.
Radiological Physics, Inc.
4333 Donnybrook Place, El Paso, Texas 79902
USA

ABSTRACT

In the wake of the events of 9/11, a presidential mandate ordered the development of a master plan to enable governmental agencies to not only seamlessly cooperate but also rapidly react to disasters. The National Response Plan (NRP) is the document in force (December 2004). It was developed to provide a framework for response to catastrophic events whether those events are natural or man-made. Homeland Security, the coordinating entity, is an integral and critical part of that plan. The NRP is a direct outgrowth of the Initial National Response Plan and operates in tandem with the National Incident Management System (NIMS). NIMS was the first real attempt to amalgamate the capabilities and resources of some 22 governmental entities, non-governmental organizations (NGOs), and the private sector.

The effectiveness of this system's response to natural disasters has been tested with reference to its performance during the 2005 late summer–early fall series of catastrophic hurricanes (Katrina, Rita, and Wilma). Ongoing evaluation of the response by the system indicates that there are significant lessons to be learned from system errors that occurred from the federal to local levels of government. Nevertheless, the conclusion would seem to be that Homeland Security's organizational structure of NMIS combined with protocols developed in the NRP represents an excellent response to both natural and man-made catastrophes.

The lessons learned in these natural occurrences (chain of command failures and missteps from first responders to national level, periodic inaccurate and irresponsible news reporting, evacuation capabilities, quarantine problems, etc.) are directly applicable to potential man-made disaster events. In the yet largely untested areas of man-made disasters, the NRP document forms the basis for responding to terrorism as well as accidental man-made related incidents.

There are two major categories of terrorism: conventional and unconventional. Conventional terrorism would include such acts as: assassination, kidnapping, hostage taking, non-nuclear explosive devices, etc. The two NRP categories of catastrophic events and oil and hazardous materials contain sections considered to be in the area of conventional terrorism. Of potentially greater immediate concern are the four major modes of unconventional terrorism that are recognized: cyber-, biological (including agro-),

chemical, and nuclear. The problem is to arrive at a mutually agreed upon order of importance of both conventional and unconventional terrorism categories. Consequent ranking of these modes enables the prioritization of those areas in which our limited national human and financial resources are to be expended and allocated (funding of research and development, commitment and selection of personnel, costs distribution, operational time-frame, information distribution level, etc.). Ranking of the terror modes will at best be difficult because of a lack of understanding of the potential impacts of each mode as well as the inherent vested bureaucratic and non-bureaucratic interests and biases.

All cases of radiation-related incidents may be considered to be manmade with a potentially significant majority of those incidents assigned to a terrorism origin. Man-made accidental occurrences would be handled with a similar NRP response as would be expected in the case of a terrorist event. Radiation-related devices include the RDDs (Radioactive Dispersal Devices) and nuclear fission and fusion weapons of mass destruction (WMD). Pragmatically, the most likely scenario to develop would involve RDD utilization. This conclusion would seem to be reasonable in view of the current apparent capabilities and sophistication required to construct, transport, and deliver a nuclear WMD.

INTRODUCTION

Over four years have elapsed since the events of September 11, 2001. That terrorist catastrophe resulted in major shifts in perception of the security of the national infrastructure by both the public and the government. The immediate resultant of that cataclysm has been the establishment of the Department of Homeland Security (DHS).[1] It was initiated by an Executive Order issued October 8, 2001. It passed into law (P.L. 107-296) on November 25, 2002. The DHS opened for business as a federal cabinet-level department on January 25, 2002. Its primary missions are, and continue to be, threefold: (1) prevention of terrorist attacks in America; (2) reduction of America's vulnerability to terrorism and homeland threats; and (3) the minimization of damage from attacks and natural disasters.[1] The impact of this anti-terrorist department has been profound and revolutionary not only in the detection, response, and mitigation of nuclear-terrorism area, but also in the related sensitive areas of bioterrorism, cyber-terrorism, agro-terrorism, and chemical terrorism. Additionally, the areas of catastrophic events, oil spills and hazardous wastes, and terrorism are covered under the umbrella of homeland security.

The presidential mandate given to the DHS was to develop a master plan with best practices and procedures to enable governmental agencies, the private sector, and non-governmental organizations (NGOs) to not only seamlessly cooperate but also rapidly react to disasters that threaten the national infrastructure. The National Response Plan (NRP) is the current major document in force (January 2005). It was developed to maintain the national infrastructure and provide a framework for response to catastrophic events, whether those events are natural or man-made. The Department of Homeland Security (DHS) and the Federal Emergency Management Agency (FEMA) are integral and critical parts of that plan. The NRP (December 2004) supersedes an earlier (9/30/03) Initial National Response Plan (INRP) document.[1] It is related to and in tandem with the National Incident Management System (NIMS)(March 2004) that represents a significant amalgamation of the capabilities and resources of governmental entities, NGOs, and the private sector.[2]

The eight fundamental infrastructures critical to the defense and economic security of the United States were defined in President Clinton's Executive Order 13010 (1996). A decade later, these remain valid today; they include: electrical power; gas and oil production, storage, and delivery; telecommunications; banking and finance; water supply systems; transportation; emergency services; and governmental operations.

HOMELAND SECURITY DOCUMENTS

While recent operations of NIMS and NRP in response to catastrophes have been less than seamless or spectacular, the fact remains that these represent a system dramatically ahead of the recorded pre-9/11 responses. These documents blueprint governmental response to natural and man made (accidental and purposeful) incidents of national concern. Natural disasters involve earthquakes (e.g., the resultant tsunami), volcanic eruptive-related activity, mass movements (e.g., landslides, catastrophic subsidence), severe weather (e.g., hurricanes, tornados), floods and fires (both are closely related to severe weather, plant cover, and topography), and extraterrestrial origin impacts (e.g., meteors).[3] The lessons learned in these natural occurrences (e.g., chain of command failures and missteps from first responders to national level, periodic inaccurate and irresponsible news reporting, evacuation capabilities, quarantine problems, etc.) are directly applicable to potential man-made disaster events. In the yet largely untested areas of made-made disasters, the NRP document forms the basis for responding to accidental and terrorism-related incidents.

The analysis and transition of the reassessment, restructuring, and reorganization of the governmental structure is well reflected by the series of homeland security presidential directives issued prior to the National Response Plan.

Homeland Security Presidential Directives

This post-9/11 series began with Homeland Security Presidential Directive 1 (HSPD-1). (Organization and Operation of the Homeland Security Council, October 29, 2001). This directive established policies for the creation of the Homeland Security Council, which subsequently developed into the Department of Homeland Security (DHS). The Council was responsible for the coordination of responses to all homeland security-related problems arising in the executive departments and agencies.

HSPD-2 (Combating Terrorism Through Immigration Policies) was issued the same day. It mandated that the Attorney General create a Foreign Terrorist Tracking Force with the assistance of the Secretary of State, Director of the Central Intelligence Agency (CIA), and other appropriate government officials.

HSPD-3 (Homeland Security Advisory System) was issued March 11, 2002. The advisory system was tasked to provide a comprehensive and effective means for the dissemination of a graduated scale of threat potential. It is recognized by the color system now in place, at each level a related corresponding set of "Protective measures" goes into force.

HSPD-4 (National Strategy to Combat Weapons of Mass Destruction [WMD]), issued in December 2002, is based on the principal "pillars" of Counter-proliferation, Nonproliferation, and Consequence Management. These pillars are integrated by four priority basis-enabling functions: (1) intelligence collection and analysis on WMD, delivery systems, and related technologies; (2) research and development to improve our ability to address evolving threats; (3) bilateral and multilateral cooperation; and (4) targeted strategies against hostile states and terrorists. HSPD-4 allows federal agencies to: (1) Deny entry to aliens associated with or suspected of being engaged in terrorism as well as (2) Locate, detain, and deport such aliens from the U.S.

HSPD-5 (Management of Domestic Incidents), issued Feb. 28, 2003, is most important. It establishes a single comprehensive national incident management system. This directive resulted in the publication of the National Incident Management Systems (NIMS) [HS, 2004a] March 1, 2004; and the National Response Plan (NRP) [HS, 2004b], December 2004. The NRP has its basis in 42 statues and regulations, 15 executive orders, and 13 presidential directives, of which 10 are specifically for Homeland Security.

HSPD-6 (Integration and Dissemination of Screening Information) issued September 16, 2003, deals with the establishment and development of a seamless terrorist database. HSPD-7 (Critical Infrastructure Identification, Prioritization, and Protection) issued December 17, 2003, deals with the basic infrastructure necessary for the system to operate. HSPD-8 (National Preparedness) issued the same day as HSPD-7, established policies for improved delivery of Federal preparedness to state and local governments.

HSPD-9 (Defense of U.S. Agriculture and Food) issued January 30, 2004, establishes a national policy to defend the agriculture and food system against terrorist attacks, major disasters, and other emergencies. HSPD-10 (Biodefense for the 21st Century) was issued April 28, 2004, and is to provide a comprehensive framework for the Nation's biodefense.

The impact of the resulting 2004 NIMS and NRP (based primarily on HSPD-5) is recognized in not only local response problems [4] but also in conventional and unconventional terrorism.[5]

National Incident Management System (NIMS)

NIMS is, in part, an outgrowth of the Firefighter's Incident Command System (ICS). The ICS system features five management areas: Command (objectives, priorities, responsibilities); Operations (conducts tactical operations, objectives, organization, and directs resources); Planning (develops action plan, collects and evaluates information, maintains resource status); Logistics (provides support and service); and Finance/Administration (monitors costs, accounting, procurement, time recording, and cost analysis). ICS developed as result of a series of recurring problems in the 1970s arising from fighting wildfires in Southern California. The system has been widely adopted by many fire departments across the nation.[6]

The NIMS document [2] provides the basis for a national standard for domestic incident management. It was developed for all levels of governmental agencies in order that they have coordinated, interoperable responses, as well as the standardization of resources. NIMS standardizes the process and procedures for incident management by aligning command and control, organizational structure, terminology, communication protocols, resources, and resource typing which enables all levels of government to efficiently respond to and recover from an incident.

National Response Plan (NRP)

The Department of Homeland Security (DHS) in December 2005 released the all-disciplines, all-hazards National Response Plan (NRP). [1] The implementation of the plan was broken down into three phases: Transition Period (60 days), Plan Modification Period (60-120 days), and Initial Implementation and Testing Period (120 days–1 year). After the first year's review, the NRP will initiate a 4-year review and re-issuance cycle.[1]

The NRP covers the full range of the complex, continually changing, interagency and multi-jurisdictional requirements, including: anticipation and response to threats or acts of terrorism and major and lesser disasters (natural and man-made incidents). It also provides a basis for mitigation and long-term community recovery. The NRP designates a chain of command and a sequence of actions from local to state and tribal to the national level of concern. It provides the basis and routes for the declaration of an Incident of National Significance (INS), which requires DHS coordination. The National Incident Management System (NIMS) (March 2004), together with the NRP, amalgamates the capabilities and resources of the governmental entities, non-governmental organizations (NGOs), and the private sector into a seamless blueprint for domestic incident management.

Catastrophic Incident of National Significance (INS) Tests

The most important aspect of NIMS and the NRP is that they respond to and are the template for major and lesser disasters of natural and man-made incidents as well as to threats or acts of terrorism. The performance effectiveness of these systems in reaction to natural disasters has been tested with its NRP catastrophic event protocol [1] during the 2005 late summer-early fall series of catastrophic Gulf Coast hurricanes (sequentially and given their estimated economic impact, Katrina [$ 40.4 billion dollars], Rita [$ 6.4 billion dollars], and Wilma [$ 10.8 billion dollars]).[7] Each of these natural catastrophes has given us lessons to be learned as well as sharpening the development of the Incident Response catastrophic system.

One term that is constantly being loosely defined, overstated, and misused is "catastrophe". It is probably most reasonably defined as an incident resulting in 1000 or more fatalities; lesser numbers of fatalities than catastrophic could be designated in several hierarchical levels of disasters. Whether or not a scale involving economic impact is necessary to the definition is debatable. Under the suggested classification, only Katrina of the 2005 hurricanes can be ranked as a catastrophe. However, Katrina is hardly comparable to the nearly coincident Muzaffarabad quake of October 8 in northeastern Afghanistan/Kashmir that resulted in an estimated 87,000 deaths. Additionally there are some 1.7 million without safe water and several hundred thousands without winter tents.[8]

Numerous problems resulted with the application of the NIMS-NRP system to Katrina. While some high-level federal glitches occurred, the major problems appear to have developed from the state-level and local-level officials who were required to trigger and place into motion local, regional, and federal level actions. The impression emerged that they were unprepared for handling the catastrophe and were apparently completely out of the loop. W. M. McClay, who served on Tulane's faculty (1987-1999), gives a reasonable analysis of problems that resulted from the hurricane's flooding including: governmental structure, media coverage, limitations of the city's location, and the cultural necessity of the preservation of New Orleans.[9]

Crisis management would seem to follow a logical sequence whether it occurs in business or in a natural catastrophe. Welch's [10] five stages of business crisis management, for example, would include: (1) Denial (when denial is no longer feasible, ironically, it often results in inertia and panic); (2) Containment (the solution of the problem is giving it to someone else = passing the buck); (3) Shame Mongering (governmental entities on all levels fight to tell their part of the story with them cast as hero); (4) Blood on the Floor (the need to satisfy the public's need for a scapegoat[s]); and, finally, (5) the Crisis is Fixed (the time when people recover and have a vision for the future). Using this approach, as an analytical tool of a crisis, enables the targeting of where the system is flawed; it is useful and certainly applicable in the case of Katrina.

Hurricane Rita, perhaps aided in part by the lessons learned from Katrina, was well handled, but clearly showed the problems encountered with the mass vehicular evacuation dilemma, a major deficiency in nearly all urban centers. Houston, and this general area of coastal southeastern Texas, has a reasonably adequate network of roads, yet gridlock resulted. The subsequent hurricane of this series is Wilma in Florida. Florida, as would be expected from its continuing experiences with hurricanes, managed NRP's protocol without significant difficulties outside of a federal entity presenting some bureaucratic problems for the state officials. It would be interesting to contrast the Wilma operation of 2005 with what took place in 2004 on the east coast of central Florida when four hurricanes in a row hit the same general area (Charles, Francis, Ivan, and Jeannie). It is most likely that multiple, sequential incidents of concern, not necessarily hurricanes, that strike rapidly and repeatedly in the same geographical area will occur in the future.

Immunity to crisis does not exist; however, the analysis of events, the response to develop needed realignments, and the necessary repairs to the system will make it stronger and more responsive. The lessons learned in these natural hurricane occurrences (chain of command failures and missteps from first responders to national level, periodic inaccurate and irresponsible news reporting, inadequate evacuation capabilities, quarantine problems, etc.) are equally applicable to man-made occurrences.

It should be noted that, while the rebuilding of New Orleans may be economically feasible, it is not geologically defensible. The location includes: an area and region of continuing subsidence, an ongoing hurricane and flood vulnerability, and, lastly, there is the fact that the lowermost Mississippi River should be flowing down the Atchafalaya River into the Gulf of Mexico not past New Orleans. Another interesting related issue of this season's hurricanes is that they display a post-Katrina event hardening of charitable giving. After Katrina and each succeeding hurricane, donations lessened. Could a similar hardening of public attitude be expected to occur after a series of terrorist incidents? We tend to forget that in modern society there are more psychological than physical victims in a catastrophe. As an example, the 3000 deaths from the 9/11 terrorist attacks also resulted in 10s to 100s of thousands of psychological casualties.[11]

Pangi [11], reviewing and utilizing the example of the impact of the Aum Shinrikyo Sarin nerve agent incident (March 20, 1995), makes use of the discipline of consequent management She analyses the psychological impacts occurring to first responders and the general public utilizing the sub-discipline of fear management. This is defined as the mitigation of panic and the management of public response following a WMD or other mass casualty incident. Panic may be defined as irrational behavior in the face of extreme circumstances.[11] Panic was certainly not a response of either first responders or the public in the Tokyo incident nor was it in the recent London subway bombing; it may be related to a question of face in Japan and a stiff upper lip in London. Acute Stress Disorder (ASD) occurs following exposure to extreme stress or trauma, but it doesn't last longer than a month.[11] Post-traumatic Stress Disorder (PTSD) is similar to ASD but it does not typically present itself until six months after the incident, usually with devastating effects on an individual's life. These aspects of the psychological consequences of catastrophic incidents will be taken under consideration in ESF-14 (Emergency Support Function) of the NRP.

The examples that we have been discussing here are catastrophic incident hurricanes. Hurricanes, as well as the bulk of natural disasters, are normally accompanied by some warning. Early warning would definitely not be expected to occur in the case of a man-made radioactive or nuclear incident. The best model for response to radiation-related incidents would be that of land-based earthquake. Marine quakes and submarine mass movements generating tsunami both come with at least a brief early warning. Earthquakes have had a long and continuous history of prediction failure. A detailed and specific review of the lessons learned in the domestic California Loma Prieta (World Series) and Northridge earthquakes may prove to be quite instructional.[3]

NRP Nuclear/Radiological Incident Annex

Taken in view of the field's long and involved history with politicians, regulators, and the public, it is not by mistake that Homeland Security has as its most detailed annex the Nuclear/Radiological Incident. This 28-page Nuclear/Radiological Incident Annex documents 6 coordinating agencies (DoD, DOE, DHS, EPA, NASA, and NRC) and an additional 17 cooperating agencies. Response coordination to an Incident of National Significance (INS) and other incidents includes: technical data management and protective action recommendation, as well as Public Information, Congressional, White House, and International data coordination. The Annex has provisions for such areas as victim decontamination and population monitoring and recovery. It has an imbedded advisory team for environment, food, and health. The concluding section of this Annex provides the chart for the responsibilities of the 22 directly affected

entities. In conclusion, the National Response Plan in combination with National Incident Management System will form the basis for combating all phases of terror (e.g., cyber, biological, chemical, etc.) on the national level.[1,2]

Man-made incidents not only include terrorism but also human-related accidents. We have been dealing with this for a considerable length of time in the production of nuclear energy. Based on the seven levels International Atomic Energy Agency (IAEA) International Nuclear Event Scale that was designed for nuclear power plant operation, what is the level in severity for the introduction of the Nuclear/Radiological protocol? Utilizing that international scale, Homeland Security would most likely become concerned at Level 3 (Serious Incident) described as having very small releases off-site, with an on-site severe spread of contamination/acute health effects to worker(s). Level 3 additionally indicates a safety defense in depth degradation as well as classified as being a near accident with no safety layers remaining. Homeland Security could be activated at Level 2 (Incident) with significant on-site impact and no off-site impact but occurring with significant failures in safety provisions. Level 1 (Anomaly) and Level 0 (Deviation) should be of no concern. The vast majority of human-related accidents occur at Level 2 or below.

Chernobyl (1986) is considered to Level 7 (Major Accident) while Three Mile Island (1979) is rated as Level 5 (Accident with Significant Off-site Risk). The implementation of the cleanup and decommissioning after the severe accidents of Chernobyl Unit 4 and Three Mile Island Unit 2 are well documented.[12] If similar future severe accidents occur either by sabotage or accident, the lessons learned in these incidents will be invaluable.

CONVENTIONAL AND UNCONVENTIONAL TERRORISM

The national infrastructure has been under direct attack by terrorism since the 1990s with a history extending back to post WWII. Terror or terrorism may be defined as violent acts made by committed groups (zealots, insurrectionists, anarchists, revolutionaries, etc.) in order to intimidate a population or government into granting their demands.

There are two major categories of terrorism: conventional and unconventional.[4, 5, 13] Conventional terrorism would include such acts as: assassination,, kidnapping, hostage taking, non-nuclear explosive devices, etc. Of potentially great immediate concern were the four original major modes of unconventional terrorism recognized: cyber-, biological, chemical, and nuclear. The problem is to arrive at a mutually agreed upon order of importance. Consequent ranking of these modes enables the prioritization of those areas in which our limited national human and financial resources are to be expended and allocated (e.g., funding of research and development, commitment and selection of personnel, costs distribution, operational time-frame, information distribution level, etc.).

The determination of this ranking would ideally be the responsibility of a panel composed of expert witnesses. What constitutes an expert witness? Invariably it is a specialist within a given field of terrorism. The problem is the expert's level of knowledge of the other three fields of unconventional terrorism. In all cases, each mode can be subdivided. In such a case, expertise may be not only being confined to an individual's portion of the mode (e.g., biotoxin and genetically modified organism experts) but also may result in confused mode cross-ranking (1 = nuclear fission devices; 2 = chemical nerve agents, 3 = biological genetically modified organisms, etc.).

At last year's Waste Management meeting (WM'05), symposium participants were asked to rank in order of their importance the four major modes of unconvential terrorism displayed on the large poster. Their reward was an 8.5x11-inch copy of the poster (Figure 1).[5] The 45 responding individuals represented a broad spectrum of foreign and domestic nuclear professionals. The responses to that rump poll (Table I)

were not anticipated (e.g., considering Nuclear Terrorism: 1 [most important] = 13%; 2 = 20%; 3 = 35%; and 4 [least important] = 31%). Utilizing the same approach, the senior author attended the U.S.–Mexico Border Health and Infectious Disease Surveillance Conference in El Paso in July 2005 with health and medical professionals (Table II). The 23 nuclear terrorism evaluation respondents this group were different (e.g., considering Nuclear Terrorism [most important] 1 = 30%; 2 = 39%; 3 = 4%; and 4 [least important] = 26%. In both surveys, biological terrorism was considered most critical.

There are some possible reasons why bioterrorism was selected as most important by both the nuclear and medical respondents informally polled. Informal impressions of the nuclear subgroup include: those over 55 trended strong nuclear and some biological; Europeans were strong on chemical (WW I memories) and biological (Mad Cow disease); and those 35 and younger were very strong for cyberterrorism. The resultant that the entire group did not consider nuclear the most critical can in part be interpreted as their not considering the RDD to be a significant terrorist weapon. The Border health specialists seem to consider nuclear more important than the WM 05 participants. Bioterrorism, as might be expected, was clearly most important. Chemical terrorism ranked consistently as second and third most dreaded. Cyberterrorism clearly ranked as least concerned.

Unconventional terrorism is a current and future concern to the nation. With four primary areas to consume personnel, resources, power, and dollars, how and on what basis are these four to be ranked in order to obtain the maximum return for the resources spent?

Any realistic evaluation of these four modes will require a risk analysis of what the subsequent impact each of these actions would have upon the national defense and the economic security of the United States. Additionally, any evaluation should include potential psychological trauma in terms of chronic and acute impacts on individuals and the local regional population as a whole. Radiation, in regards to human health, for example, will require a realistic evaluation of the immediate, short-term, long-term, and generational physical health impacts. Transparency of all operations is absolutely necessary to prevent scripted and inadvertent chaos and hysteria.

What would seem to be required are experts with a broad understanding of the entire spectrum of unconventional terrorism. Failure to accomplish this will result in a purely political process rather than an expert-driven selection process.

RE-RANKING UNCONVENTIONAL TERRORISM

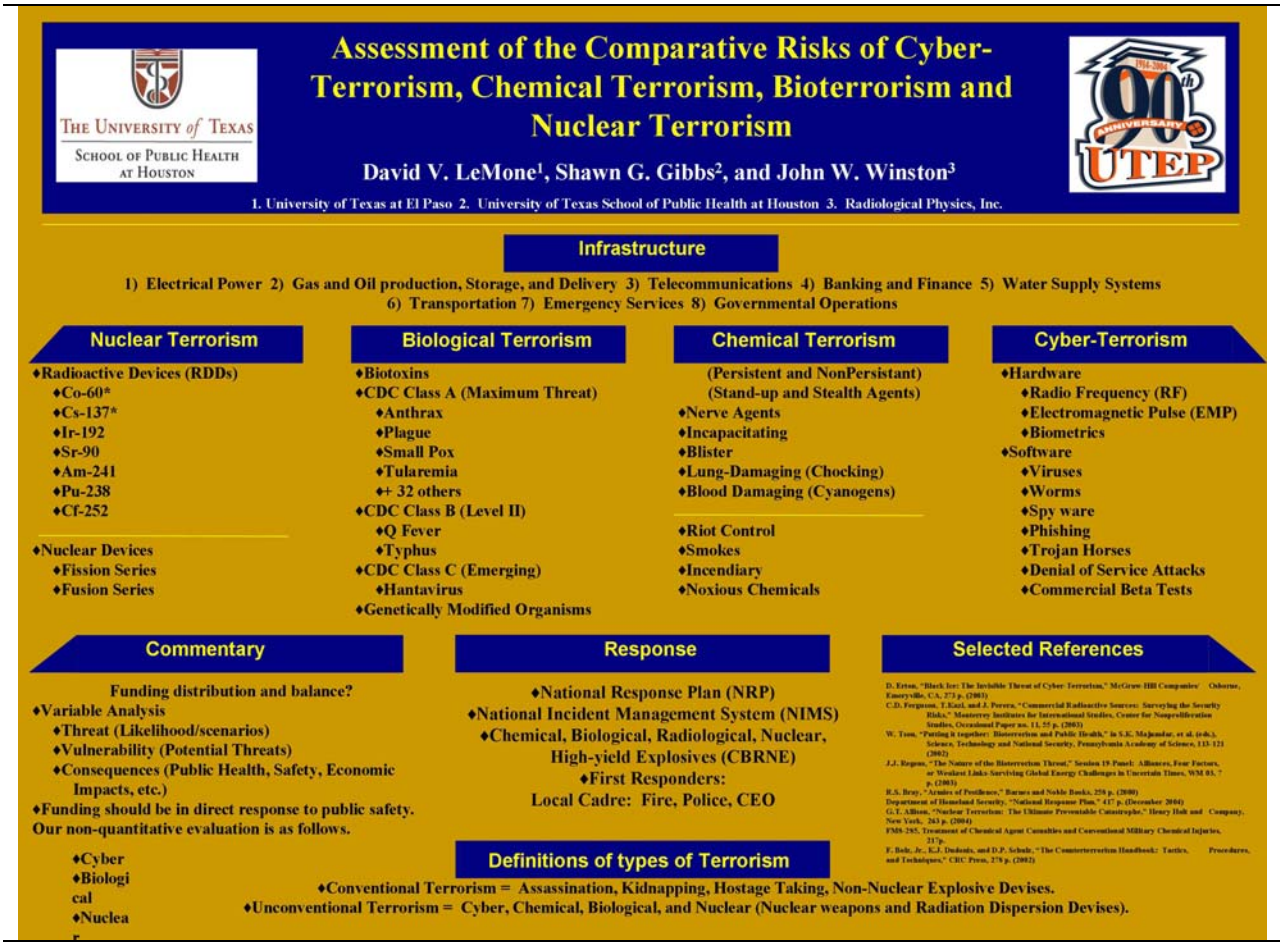

Fig. 1. Chart

Table I. 31st Annual Waste Management Symposium, Tucson, AZ

MARCH 2, 2005 INFORMAL RANKINGS OF UNCONVENTIAL TERRORISM 45 SYMPOSIUM RESPONDENTS				
	BIOLOGICAL	CHEMICAL	CYBER–	NUCLEAR
Most concern 1	35%(16)	17%(8)	31%(14)	13%(6)
2	35%(16)	35%(16)	8%(4)	20%(9)
3	17%(8)	26%(12)	20%(9)	35%(16)
Least concern 4	11%(5)	20%(9)	40%(18)	31%(14)

Table II. US-Mexico Border Health and Infectious Disease Conference

CAMINO REAL — EL PASO, TEXAS JULY 28, 2005 INFORMAL RANKINGS OF UNCONVENTIAL TERRORISM 23 SYMPOSIUM RESPONDENTS				
	BIOLOGICAL	CHEMICAL	CYBER–	NUCLEAR
Most concern 1	39%	4%	26%	30%
2	21%	52%	13%	13%
3	30%	39%	4%	30%
Least concern 4	8%	4%)	56%	26%

The National Response Plan (NRP) subdivides the incidences of national concern into eight areas, both conventional and nonconventional. Conventional designation would include: Catastrophic (natural and man-made [accidental and planned]); Oil and Hazardous Materials; and the category of Terrorism. Unconventional terrorism remains the same with Biological, Chemical, Cyber-, and Nuclear/Radiological. The inclusion of Agroterrorism into Bioterrorism is subject to debate. The division of radiation-related terrorism into two categories, Nuclear and Radiological, is less problematic.

Nuclear/Radiological

Given the possibility to poll the participants again on the original document (Figure 1), Nuclear Terrorism would be subdivided into two clearly defined areas of unequal weight and concern: Radioactive Devices (e.g., RDDs) and Nuclear Devices (Fission and Fusion series).[4, 5, 13] This is predicated on the evidence of Khan's nuclear black market dispersal of high-speed cascading ultracentrifuge data as well as other sensitive technologies.[14] An additional interesting sidelight to this development is the fact that the basic source material, yellow cake uranium oxide, has recently spiked in a rise from a long-term price level around $8.00/pound to $33.25 (29.50 Euros) on the Canadian market (www.uxc.com/review). Uranium solution-based and hard rock mining activity seems to be developing in response to the increasing demand for this commodity.

It should also be recognized that phosphates, a very abundantly distributed global agricultural resource, are capable of being processed for the recovery of uranium and thorium. Thorium based fuels are appropriate for a nuclear power plant fuel in pressurized water reactors as well as high temperature gas-cooled reactors (pebble bed THTR-300). This fuel has a long record of reactor experimental use. Thorium (Th-232) based fuel has the advantage of producing fissionable U-233 instead of weapons grade-usable Pu-239, which is the product of a neutron and an atom of U-238, that would be developed in normal U-235 and U-238 fuels.[15]

Radioactive devices have been and are much more easily constructed, developed, and delivered than the nuclear devices. The resultant of a radiation dispersal device (RDD) is more of a problem of prohibitive cleanup cost rather than acting as any kind of effective lethal or psychological piece of equipment.[LeMone RDD] It should be noted that one of the potential ingredients for a RDDs would be Cs-137. Experience with a 1987 Cs-137 accident in Goiana, Brazil, has revealed that Prussian Blue was successfully utilized in the treatment of contaminated individuals.[16] Prussian blue side effects include

constipation, stomach pain, and blue-colored feces. Regional stockpiles should have these pills in their inventory. In the event of an attack by a RDD or by an improvised nuclear device, the risk levels for radiation cleanup are critical. They cannot be set at such a high level that they become prohibitively expensive.

Given the rigorous controls and in-depth safety systems, we consider the possibility of a nuclear power plant disaster with off-site releases as a very unlikely concern. It does not preclude the possibility of either an accident or sabotage. To address the possibility of an off-site release, there were to be potassium iodide pills distributed to everyone within a 20-mile radius to any nuclear power plant. The purpose of the pills is preventing the thyroid gland of children and young adults from absorbing radioactive iodine. These pills should have been distributed in 2003 and are slated for availability in 2006.[17]

Conversely, a nuclear device is neither easily constructed nor developed without difficulty even by highly sophisticated engineers and scientists. Additionally, the delivery of a nuclear device either by missile or other means by stateless transnational terrorists presents an almost impossible task. However, nuclear devices will have a much larger negative economic impact; they are significantly more lethal; and they are a psychologically devastating effect in both the long and the short term. In view of global conditions, the potentiality of a delivered nuclear device can no longer be ruled out as being impossible.

Agroterrorism

The NRP treats Agroterrorism as a separate entity from Bioterrorism. Agriculture and the food industry is the softest of all the transnational terrorist's targets. It lays the country open to a devastating blow to those in a largely urban society dependent upon others for their food supply. Agroterrorism places at risk ranches, farms, food processing plants, animal feed lots, etc.[Pearlstein] The problem is in part the rise and continuing growth of agribusinesses. Some selected results of that development are: seed suppliers in very limited locales, highly centralized farms, lack of crop diversity, and the overuse of herbicides and antibiotics.

In the United States it should be noted that food imports annually occur through 132 ports with around 30 billion tons of material being sent in 3.7 million separate shipments. Around 150 Food and Drug Administration (F.D.A.) inspectors inspect these imports.

Da Silva [19], as an example of bioterrorism potential, cites 1996 [20] data where between 6.5 and 33 million cases arise annually from food pathogens, resulting in 9000 fatalities. The cost of this is estimated at between 2.9 and 6.7 billion 1996 dollars annually and is attributable to six common bacterial pathogens found in animal products (*Salmonella typhosa, Campylobacter jejuni, Escherichia coli 0157H:H7, Listeria monocytogenes, Staphylococcus aureus,* and *Clostridium perfrigens*).[19] Significant losses of vegetable and fruit exports are attributable to fungal and bacterial diseases. Deliberately or legacy contaminated food containing herbicides, pesticides, or heavy metals residues as well as the use of arable cropland for growing ornamental plants and cut flowers, add to an overall insecurity about the system. Pearlstein's [18] case-in-point was the February 1978 liquid mercury contamination of Israeli oranges which resulted in major economic losses to their citrus industry.

Anticrop biowarfare has included such diverse targets as sweet potatoes, soy beans, sugar beets, cotton, wheat, and rice while utilizing biological agents (yellow and black wheat rusts, anthrax, late blight of potatoes, etc.) and insects (e.g., Colorado, rapeseed, and corn beetles). Britain and the Soviet Union were involved in anti-crop and anti-livestock weapons for use against Nazi Germany. According to Alibek [21], the directorate known as Ecology developed: foot and mouth disease and rinderpest for cattle; African swine fever for pigs; and ornithosis and psittacosis for poultry. These agents were designed to be

sprayed from a bomber flying low across farmlands in a straight line in order to contaminate a large area. Sporadic outbreaks along this line could eliminate agricultural activity over a wide area.

The Food and Agriculture Information Sharing and Analysis Center (ISAC) established guidelines for responsibility in the agricultural and food system area. These guidelines include: detecting potential threats to the critical infrastructure, assessing threat information, providing timely warnings to the critical infrastructures so countermeasures can be developed and implemented, and responding in the event of a terrorist attack. The president sent a mandate to Homeland Security (HSPD-9) to develop a national policy for the agriculture and food system, including defense of the system against terrorist attack, major disasters, and other emergencies, on January 30, 2004. That policy was still in development and was not included in the National Response Plan issued December 2004. The conclusion would seem to be that Agroterrorism is complex and critical enough to be elevated from a subcategory; the same could be said for other bioterrorism subdivisions. Nevertheless, the judgment of Homeland Security is to elevate Agroterrorism to the same level as bioterrorism and the other unconventional terror entities.

Bioterrorism

Biological warfare is defined as the utilization of living organisms (plants, fungi, bacteria, etc.) and/or their toxins to harm, incapacitate, or exterminate an adversary's military forces, civilian population and flora and/or fauna, including livestock [22.]. This can be accomplished by utilization of any naturally occurring living organism, including the modern genetically modified ones, and/or bioactive substances. These, consequently, may be delivered either by increasingly proliferating conventional warheads [23] or by less technologically advanced civilian delivery means (e.g., anthrax through the mail system).[24]

Bioterrorism is widely considered to represent the most serious threat from unconventional approaches.[5] Regen [25] enumerates four primary factors to be determined when arriving at an evaluation of the bioterrorism threat: first, are there increasing numbers of nations involved in processing, seeking, or acquiring biological weapons; second, production of genetically modified organisms (GMOs); third, detection of biowarfare development is difficult to establish, because the research is intertwined with agriculture and medicine; and lastly, applied bioagents may not only have incubation periods of only days but they may be difficult to diagnose. However, bioweapons, like chemical weapons, are commonly forensically traceable.[5]

Man's history of the last 5 millennia has been intimately involved with sequences of pestilence (e.g., plague, malaria, typhus, yellow fever, smallpox, cholera, influenza) that have resulted in revolution, war, and the destruction of societies as well as political systems [26, 5]. A modern world consisting of over 6 billion individuals with transport capability of going anywhere globally in 36 hours or less makes timely prevention of disease transmission by quarantine range from extremely difficult to a nearly impossible priority.

The NRP, in its disaster control function, is supposed to handle the periodically occurring natural global pandemics, as well as bioterrorism. Today, the publicized threat of a global spread of a zoonotic (animal to man) Asian bird flu has not only added the term pandemic to the public's general vocabulary but also developed considerable effort in the biomedical sciences. Knapp [27] points out that the current variants of hepatitis, HBV (hepatitis B virus) and HCV (hepatitis C virus) represent a significantly larger immediate problem for the estimated 1.5 billion HBV infected worldwide. First identified in 1967, HBV is a large complex virus with its highest levels being recorded in sub-Saharan Africa and East Asia. HBV infections are transmitted: vertically (mother to child), horizontally (child to child), by risky sexual behavior, reused needles, and infected blood supplies.

HCV, a close cousin to the dengue and yellow fever viruses, has a simpler molecular design and is far more deadly than HBV. The disease results in greater than 50% fatality rate, frequently involving liver cancer and cirrhosis. It is estimated that 250,000 have contracted the virus.[27] The HCV zoonotic mutation apparently developed in WWII with large numbers of Japanese troops in China, Southeast Asia, and those repatriated to Japan. Veterans of the French and Indochina wars are believed to be the vectors to the western world. Anti-viral treatment and liver transplants are described as prohibitively expensive and highly unsatisfactory. Use of either HBV or HCV as a bioweapon seems unlikely due to its 20-30 year lag time. However, it poses a long-term social and financial threat that will lead to future political instability. Knapp [27] also points out that the numbers affected by less-supported HBV/HCV viruses (nearly two billion) are much higher than the HIV affected (30 million).

Of greatest current consideration is the natural catastrophe generated by a potential pandemic threat of a zoonotically derived human transmissible Avian flu (H5N1 virus). Economists see the likelihood of a major pandemic improbable; however, they make predictions as to its market impact, if it should occur (Citigroup Investment Research).[28] If the virus mutates to a humanly transmissible form, they predict either a mild or virulent pandemic with economic ramification in either case. If it is a mild pandemic, such as the SARS outbreak that was largely confined to Hong Kong, China, Singapore, and Japan, expect 2-7 million fatalities (World Health Organization [WHO] data). The SARS example depressed the Asian productivity and markets with falls ranging from 7%-17%.[28] Stock market winners in this situation were drug companies (anti-viral drugs and vaccines), hospital chains, home-entertainment providers, cleaning product makers, and telecommunications. A protracted, virulent pandemic, utilizing the 1918-1919 Spanish flu as a template, would result in a fatality count between 20 and 100 million (WHO). The result would include global economic decline, raw material source collapse, easing of monetary policies, and falling interest rates.[28] The NRP addresses this potential natural catastrophe in its annex on biology.

CHEMICAL TERRORISM

Chemical terrorism has a long and reasonably stable list of agents that may be used as weapons.[5] These agents kill, maim, debilitate (acutely and also chronically), and may have serious genetic implications. Chemical agents are typically liquid and dependent on their volatility and rates of reaction for effectiveness. Therefore, such natural conditions as the surface they are deposited on, temperature, humidity, wind direction, and wind velocity are critical to their dispersal. Normally chemical agents are heavier than air and have a tendency to drain into lower topography.

Chemical agents may be broadly classified on the basis of the reactions they elicit to the human system as: nerve, blister (vesicant), and choking (pulmonary irritants) [29]. Nerve agents disrupt the muscle functions of the body. Large doses are lethal and are preceded by a tight chest, blurred vision, nausea, convulsions, and coma. Nerve agents are listed into a G series: GA (tabun), GB (sarin), GD (soman), and GF (cyclosarin), named for the German teams that created them during and shortly after WW II. The second somewhat oily nerve agents are listed in the V series (VE, VG, VM, VX). These agents are 10 times more toxic than sarin (GB) and are persistent agents (not easily degraded or washed away).[30]

The three common blistering (vesicant) agents are: mustard gas, lewisite, and phosgene oxime. Mustard gas was used extensively in World War I (WW I). It resulted in blistering on exposed body parts as well as affecting the internal organs. Blindness usually preceded respiratory failure and death. Choking (pulmonary irritant) agents form the third group. They are typified by chlorine and phosgene gases, which damage the respiratory system. These gases first appear as minor irritants and are followed 4-5 hours later by pulmonary edema, which fills the lungs with water and results in suffocation. Phosgene has been cited for 80% of the American chemical fatalities in WW I.[29, 31]

Rieders [32] divides chemical weapons into two major categories: "stand-up" chemical weapons and "stealth" chemical weapons. The "stealth" or delayed bio-impact agents produce a delayed toxicity. These agents (toxic bio-transformers) are activated by the body's metabolic processes. Chemical weapons invariable leave unique "chemical finger prints". An excellent example is Yeso Seto's [38] identification of the nerve gas (GB sarin) used in the 1995 Tokyo subway attack. These data were instrumental in the identification of the Aum Shinrikyo, an international doomsday terrorist cult.[29] These chemical agents have thickeners to increase the viscosity and stickiness, stabilizers to prevent early release, and carriers to aid in distribution. Additionally, additives such as the reagents in which the agent is dissolved in, aerosols, explosive agents, and penetrators (for breaching clothing and skin) are forensically traceable elements. Nation states and/or organizations forensically proven to be involved in chemical terrorism invite a retaliatory response.[32]

After World War I, the 1925 Geneva Protocol (Rules of War) prohibited further use of chemical and biological weapons (the protocol was never ratified by the United States), and has long been ignored by terrorist organizations. All of these chemical weapons are now classified as weapons of mass destruction (WMD) (UN Resolution 687). The production and stockpiling of chemical weapons was outlawed by the Chemical Weapons Convention of 1993 (brought into force 4/29/97).[30] Chemical terrorism does not have an independent NRP Annex. It is referred to in the Oil and Hazardous Materials Incident Annex Scope as a hazardous material (WMD chemical agents). It is also referred to within the Planning Assumptions and Considerations of the Terrorist Incident Law Enforcement and Investigation Annex as chemical materials.

CYBER-TERRORISM

Cyber-terrorism is defined as the execution of an attack to disable, disrupt, or destroy a nation's critical electronic information infrastructure. With the now-universal utilization of the Internet, the question of information security is of paramount concern.[5] The central problem encountered in cyber-terrorism is in the software utilized. Mossberg (2004) [34] notes that significant software development is being outsourced (India, China, etc.).

After 10s of billions of dollars were spent on the sales of Windows-based software and operating systems, it appears that they come without adequate security measures, resulting in the development of a myriad of viruses and spyware systems. Symantec has estimated 50 new software vulnerabilities/week and 100 new viruses/week.[35] In 2003-2004, the estimated costs to businesses of the six major viruses (Sasser, NetSky, MyDoom, SoBig, Blaster, Slammer) was placed at 17 billion dollars.[36] The money and effort spent correcting these internal flaws is deplorable. It has, however, given rise to a cottage industry engaged in securing and patching the systems. Apple-based systems are considered by many to be more secure and superior; however, their activity accounts for only 2% to 5% of the usage.

Viruses and worms are mostly distributed by E-mail and are the result of malicious intent, ego-tripping, or criminal purpose. Some viruses on PCs will infect vulnerable systems by attacking known network software vulnerabilities. Still others attack unsuspecting users through malicious web sites.[42]

Spyware and phishing, both of which are web-based vulnerabilities, has introduced a new method of potential criminal and terrorist utilization.[38] Spyware programs monitor a user's keystrokes to steal information (e.g., passwords). Phishing for credit card data involves the "hijacking" of a web site in order to steal their identity so that when a user posts confidential information on it, the data are revealed. "Mimicking" has been suggested as a more accurate term than phishing. The phenomenon has been growing at an alarming rate.

Wireless networking has visibly been taking over the market with projected sales of 27.7 million for

2005.[Buckeley] Popular, low cost wireless networking connecting with mainframe computers evolved from the old hard-wired desktops to easily secured mobile laptops, initially using modems and phone lines and evolving to the wireless systems of today. Unfortunately, wireless probes (beacons) do not distinguish between authorized and unauthorized users. The result has been that some formerly secure corporate systems are being breached. Additionally, this technology allows drive-by viruses to be sent from a laptop to a computer.[42] The hacker at the airport, sitting with his laptop, could be probing for your passwords and credit card data. Unfortunately, there are major security flaws in wireless communications. Major industry players, as well as developers, are working to resolve this, but they still lag behind the dynamism of the system developing under current technology.

As discussed earlier [5], the world of this century is a globally integrated web of international businesses, corporations, and financial institutions. The Internet data that are transmitted by these entities are vulnerable to such scenarios as: network flooding ("denial of services"), intrusions into corporate intranets, threats, attacks (both directly and as Trojan horses), and viruses. [39] Properly confined, hardened secure systems are, in general, enough; however, attackers are constantly developing new technologies and discovering new vulnerabilities, making security an ever changing process, not an end.

Additionally, the vulnerability of the physical layer connecting systems to the internet occurs with the detonation of a strong atmospheric nuclear blast which generates an electromagnetic pulse (EMP). This pulse is capable of knocking offline, either temporarily or permanently, both unprotected computer systems and network components.[40]

The nine cooperating agencies of the critical NRP Cyber Incident Annex are developing a coordinated, broad-based, multidisciplinary plan to prepare for, respond to, and recover from cyber-related impacts.

CONCLUSIONS

In the evaluation of Homeland Security's work, we can say that the responses to the three major hurricanes of 2005 by the disaster response framework established by NIMS and the NRP were not without problems. Overall, however, the experience of the then forming NRP definitely provided a positive result to selected protocols used and, conversely, pinpointed those protocols heretofore poorly defined. The NRP became the national standard playbook for disaster response as of January 2006.

Nuclear events need to be divided into separate Radioactive (RDDs) and Nuclear (WMD) modes. The most serious and disturbing development is the continuing inability to control the proliferation of nuclear weapons of nuclear mass destruction. Nuclear events in both categories will come without warning. In evaluating global natural disasters the best response to nuclear events would seem to be terrestrial seismic analogs (earthquakes); they have never been predictable with any sort of accuracy in time, location, or strength. They, therefore, provide for the nuclear category the best source of lessons learned in natural disasters. Nuclear devices (WMDs) also benefit from the records developed from Hiroshima and Nagasaki events of WWII. Terrestrial and marine mass movements are seldom predictable. Conversely, meteor impact, as well as weather-related phenomena, provide forewarning and predictability. Other disasters, such as earthquake-generated tsunami, are monitorable and may give some lead-time to the disaster at a distance. Volcanoes are also somewhat predictable when monitored for seismic activity and swelling.

Agroterrorism has been separated from bioterrorism [NRP] and elevated to the status of the other five major unconventional terror areas, thereby further complicating the process of deciding where to expend the personnel, resources, and finances of the government in the future. Additionally, each of these six modes needs to be evaluated and ranked not only for the physical damage consequences (casualties and infrastructure damage) that occurs but also for the psychological impact to the populace [Pangi].

Given the opportunity to make a single comment about the problem of terrorism, it would have to be that while our society is far too complex and interconnected to defend against all possible threats, we can at least prepare for these threats in part By utilizing what we learn from natural disasters. The National Response Plan developed by Homeland Security has given us a reasonable roadmap of how to respond on all governmental levels to both natural and manmade disasters.

REFERENCES

1. HOMELAND SECURITY, "National Response Plan, (NRP)," December 2004, 426 p. (2004b)
2. HOMELAND SECURITY, "National Incident Management System (NIMS)," March 1, 2004, 193 p. (2004a)
3. P. L. ABBOTT, "Natural Disasters," 5th Edition, McGraw-Hill, New York, 496 p. (2006)
4. D. V. LEMONE, S. G Gibbs, and J. W. Winston, "The Problem of Local Response and Mitigation to Nuclear Radiation Dispersal Devices ("Dirty Bombs") and Sabotage Incidents," Session 22, (5179) Radiological Dispersion Devices, Response and Cleanup in Emergency Radiological Situations, Waste Management '05, 11 p., (2005).
5. D. V. LEMONE, S. G Gibbs, and J. W. Winston, "Assessment of the Comparative Risks of Cyber-Terrorism, Chemical Terrorism, Bioterrorism, and Nuclear Terrorism," Waste Management 2005, Session 33, (5180) Environmental Remediation, Special Wastes, and Public Communication, 15 p. (2005).
6. INCIDENT COMMAND SYSTEM, "National Training Curriculum, ICS Orientation, Module I, Reference Text," National Interagency Fire Center, NFES-2439, 28 p.
7. G. STEIN, "Triple-Whammy Storms Cost Insurers 57.6 Billion Dollars," El Paso Times, v.125, no. 362, F-1 (2005)
8. WONACOTT and Z. HUSSAIN, "Politics Hinge Earthquake Aid," Wall Street Journal, v. 246, no. 112, A-14 (2005)
9. W. M. McCLAY, "Storm over Katrina," Commentary, vol. 120, no. 5, p. 31-41(2005)
10. J. WELCH, "The Five Stages of Crisis Management," Wall Street Journal, Opinion, (9/14) v. 246, A-20 (2005)
11. R. L. PANGI, "After the Attack: The Psychological Consequences of Terrorism," in J. N. Kayyem and R. L. Pangi (eds.), "First to Arrive: State and Local Responses to Terrorism," MIT Press, Cambridge, Massachusetts, p. 135-162 (2003)
12. INTERNATIONAL ATOMIC ENERGY AGENCY, "Cleanup and Decommissioning of a Nuclear Reactor after a Severe Accident," Technical Report Series 346, Vienna, 59 p. (1992)
13. D. V. LEMONE, "Sealed Radioactive Sources (SRS) and Greater Than Class C (GTCC) Low-Level Wastes: Potential Radioactive Dispersal Devices (RDD) Resources," Waste Management '04, Session 55, (4525) Management of Spent and Disused Radioactive Sealed Sources, 15 p. (2004)
14. G. T. ALLISON, "Nuclear Terrorism: The Ultimate Preventable Catastrophe," Henry Holt and Company, New York, 263 p. (2004)
15. M. S. KAZIMI, "Thorium Fuel for Nuclear Energy," American Scientist, vol. 91, no. 5, p. 408-415 (2003)
16. INTERNATIONAL ATOMIC ENERGY AGENCY, "Dosimetric and medical aspects of the radiological accident in Goiania in 1987," IAEA-TECDOC-1009, Vienna (1998)
17. M. HALL, "Nuke Pills Not Ready Despite '03 Deadline," USA Today p.1A (2005)

18. R. M. PEARLSTEIN, "Fatal Future," University of Texas Press, Austin, 198 p. (2004)
19. E. J. Da Silva, "Biological warfare, biodefense and the biological and toxin weapons convention," Nature Biotechnology, vol. 2, no. 3, 17 p.(1999)
20. J. C. BUSBY, T. Roberts, C-T Lin, and J. M. MacDonald, "Bacterial food-borne disease medical cost and productivity losses," Agricultural Economic Report, no. 741, 80 p., Economic Research Report, U.S. Department of Agriculture, Washington, D.C.(1996)
21. K. ALIBEK, "Biohazards, the chilling true history of the largest covert biological weapons program in the world," Random House (1999)
22. R. K. CHADURI, D. C. Pal, and I. Chaduri, "Plants and Toxins as Biowarfare Weapons," in S. K. Majumdar, et al. (eds.), Science, Technology and National Security, Pennsylvania Academy of Science, p. 30-46 (2002)
23. J. C. MOLTZ, "New Challenges in Missile Proliferation, Missile Defense, and Space Security," Monterrey Institute for International Studies, Center for Nonproliferation Studies, Occasional Paper No. 12, 72 p. (2003)
24. S. K. MAJUMBAR, J. H. Tchaicha, A. C. Donaghy, and C. M. Marc, "Biotechnology and Biological Warfare: A Review with Special Reference to the Anthrax Attack in the U.S.," in S. K. Majumbar et al. (eds.) Science, Technology and National Security, Pennsylvania Academy of Science, 10-29 (2002)
25. J.J. REGENS, "The Nature of the Bioterrorism Threat," Session 19-Panel: Alliances, Fear Factors, or Weakest Links - Surviving Global Energy Challenges in Uncertain Times, WM 03, 7 p. (2003)
26. R.S. BRAY, "Armies of Pestilence," Barnes and Noble Books, 258 p. (2000)
27. A. B. KNAPP, "The HVB and HCV Pandemic: Health, Political, and Security Challenges," Political Science Quarterly, vol. 120, no. 2, p.243-251 (2005)
28. M. R. SESIT, "Gloomy Science: a look at Avian Flu, Wall Street Journal, v. 246, no. 113, C-12 (2005)
29. F. BOLZ, JR., K.J. DUDONIS, AND D.P. SCHULZ, The Counterterrorism Handbook: Tactics, Procedures and Techniques, CRC Press, 278 p.
30. WICKIPEDIA, http://en.wickipedia.org/wiki/Nerve_gas
31. R. F. KNOUSS, Inside and Outside the Loop: Defining Population at Risk in Bioterrorism, in J. N. Kayyem and R. L. Pangi (eds.) First to Arrive, MIT Press, Cambridge, p. 121-134 (2003)
32. M.F. RIEDERS, "Issues in Homeland Security: Forensic Evidence in Real or Perceived Exposure to Chemical substances," in S.K. Majundar, et al. (eds.) Science, Technology, and National Security, Pennsylvania Academy of Science, Chapter 4, p. 47-61 (2002).
33. W. S. MOSSBERG, "Personal Technology," Wall Street Journal, B-1, 12/2/04 (2004)
34. D. BANK a, "Bush is Pressed to Boost Security on Information–Technology Front," Wall Street Journal, p. A3, A10 12/7/04, (2004)
35. C. BRYAN-LOW AND L. ROUSEK, "Police Target Sensitive 29A' Virus Creators," Wall Street Journal, B1, B7, 12/2/04 (2004)
36. D. BANK b, "Keeping Information Safe," Wall Street Journal, B-1, B-6, 11/11/04 (2004)
37. W. M. BUCKELEY, " Wireless Mischief," Wall Street Journal, B-1, B-6 (2004)

38. Y. SETO, "Sarin Gas Attacks in Japan and Forensic Investigations - A case Report" in S.K. Majumdar, et al. (eds.) Science, Technology, and National Security, Pennsylvania Academy of Science, Chapter 5, p. 62-73 (2002).

39. J. OMURA, J. SPILKER, Jr., and P. BARAN, "The Evolution of Modern Digital Communications Security Technologies," in S.K. Majumdar, et al. (eds.) Science, Technology, and National Security, Pennsylvania Academy of Science, Chapter 15, p. 160-185 (2002)

40. C. WELDON, "Overview: Preparing America for the 21st Century," in S.K. Majumdar, et al. (eds.) Science, Technology, and National Security, Pennsylvania Academy of Science, p. 1-9 (2002)

41. D. ERTON, "Black Ice: The Invisible Threat of Cyber-Terrorism," McGraw-Hill Companies, Osborne, Emeryville, CA, 273 p. (2003)

42. D. NASOW, "Command Centered Launched to Fight Instant-Message Viruses," Wall Street Journal, D-8, 12/7/04, (2004)