



Center for Nonproliferation Studies
Monterey Institute of International
Studies

Bioterrorism Threat Assessment and Risk Management Workshop

FINAL REPORT AND COMMENTARY

Presented to the U.S. Department of Energy

June 24, 2003

by

Raymond A. Zilinskas (Rapporteur)

Bioterrorism Threat Assessment and Risk Management Workshop

FINAL REPORT AND COMMENTARY

1. Introduction

A 1½ day-long workshop on bioterrorism threat assessment and risk management was held during November 12-13, 2001, at the Washington, D.C. office of the Center for Nonproliferation Studies (CNS), Monterey Institute of International Studies. Twenty-two experts from academe, industry, and government participated in the workshop. The intent of this multi-disciplinary workshop was to bring together risk assessment/risk analysis practitioners with experience in biotechnology, environmental sciences, the insurance industry, the pharmaceutical industry, public health, and space biology with security and intelligence threat analysts to stimulate an initial exchange of ideas and information on lessons learned that could be useful to both communities. The organizers in particular hoped that this exchange would lead to the generating of useful ideas that subsequently would be applied to develop new or improved risk assessment methodologies to assist government agencies in planning effective counterterrorism policy and bioterrorism consequence management.

This is the report of the workshop. It has two sections: (1) a short background in which the issue in question is presented and the workshop's objective is defined, and (2) a section in which the organization and agenda of the workshop are described, along with its findings. Appended to the workshop report is a short paper, authored by several workshop participants, that contains: (1) a commentary on workshop proceedings and findings, and (2) recommendations for follow-up activities to the workshop. In addition, there are two annexes; Annex 1 lists the participants of the workshop, while Annex 2 lists the participants of a subsequent meeting held on March 27, 2003, in Livermore, California.

2. Background to the Workshop

Before the workshop was held, the workshop organizers had prepared a Background Paper (Homsy and Zilinskas, 2001), a copy of which was presented to each workshop participant before the workshop commenced. In the Background Paper are defined terrorism, bioterrorism, and biocriminality, as well as terms such as "threat analysis;" "risk assessment;" and "risk management;" and the problem is stated; i.e., is it possible to do an objective assessment of the risk of bioterrorism? The Background Paper also had four annexes. Annex 1 contained a short discussion of four pertinent biological events; Annex 2 consisted of a list of critical biological agents as defined by the Centers for Disease Control and Prevention (CDC); Annex 3 had a glossary of risk analysis terms; and Annex 4 listed pertinent references to citations in the text. Except for information in the following section, material covered in the Background Paper is not restated in this report.

Before preparing the Background Paper, the workshop organizers were well aware that there had been calls for the development of rigorous analytical methods to assess the risks of bioterrorism. Most notably, in September 1999, the U.S. Government Accounting Office (GAO) issued a report in which it strongly recommends that such methods be developed by the Federal Bureau of Investigation (FBI) for use in assessing bioterrorism risks (Government Accounting Office 1999). Further, Comptroller-General David M. Walker, head of the GAO, testified before

Congress that drawing up a comprehensive assessment of likely terrorist threats “has become an urgent imperative” (Broad 2001).

This issue was again the subject of a Congressional hearing on October 12, 2001, when the House Subcommittee on National Security, Veterans Affairs, and International Relations addressed the topic “Combating Terrorism: Assessing the Threat of Biological Terrorism.” In particular, it sought to examine “the factors that should be considered in assessing the risks of biological terrorism.” Witnesses at the hearing made clear the necessity of developing robust risk assessment methodology applied to bioterrorism.

However, to date the GAO’s counsel has not been followed. Reportedly, on September 20, 2001, a member of the House Subcommittee on National Security, Veterans Affairs, and International Relations asked FBI counterterrorism officials about the status of the process to develop new threat and risk assessment methodologies. They answered “they knew nothing about the assessment” (Palarino 2001). Further, the Office of the Inspector General issued a report in September 2002 that states, “The FBI has never performed a comprehensive written assessment of the risk of the terrorist threat facing the United States” (Office of the Inspector General, 2002). As this workshop report is being revised in May-June 2003, the rapporteur has been unable to find any substantive signs that either the GAO report or the subsequent hearings have resulted in any improvements to risk assessment methodology related to bioterrorism.

Given this context, and in view its mission to develop technology to address terrorist threats, the Chemical and Biological National Security Program (CBNP), within the National Nuclear Security Administration of the U.S. Department of Energy (DOE), decided to investigate whether analytical methods used in disciplines outside the intelligence and security communities might have applications in efforts to identify and prioritize cost-effective investments in defenses against bioterrorism¹. Accordingly, it tasked the Lawrence Livermore National Laboratory and the CNS to convene an interdisciplinary workshop to consider if it is possible to perform a rigorous risk analysis of terrorist use of biological weapons to generate mass casualties (e.g., more than 1,000 victims) and, if this was possible, to determine how such a risk analysis should be performed.

3. Workshop Activities and Findings

During the first day, experts in decision and risk analysis (encompassing the sub-disciplines of risk assessment, risk communication, and risk management) made presentations on how quantitative risk analysis methods have been applied in other fields where critical decisions must often be made under conditions of considerable uncertainty. Such fields include public health, nuclear power, space program planning, environmental protection, and facility security. During the first day, the workshop also heard presentations from experts on bioterrorism and from representatives of law-enforcement agencies.

On the second day, the workshop was divided into three breakout groups, each of which was comprised of a mixture of expertise from various disciplines. Each breakout group was asked to come to a consensus on three issues:

¹ The DOE /NNSA CBNP, which is chartered with developing technologies and systems to address chemical and biological threats to civilian populations, was transferred to the new Department of Homeland Security (DHS) on March 1, 2003. The DOE interest in risk-based prioritization in this context, except for the need to protect its own facilities against biological threats, has been assumed by an expanded program within DHS.

- Was it possible to lay out a coherent framework for risk assessment/risk management to address bioterrorism threats and, if it were possible, what would the framework look like?
- Was it possible to identify key variables for risk assessment/risk management and determine where data may be lacking?
- Was it possible to describe an outlook for the proposition: what do we need to know that we do not know?

Although the breakout groups worked separately, the results of their deliberations were similar. Thus, they came to the following two major conclusions:

1. There is a need to identify a hierarchy of threats related to bioterrorism (this is in effect an assessment of threats posed by bioterrorists). Each bioterrorist threat has different attributes that depend on:
 - Intent or goals of the group or individual; i.e., the motivation for the group or individual's actions, including the willingness to employ weapons of mass destruction.
 - The technical capabilities of the group or individual; i.e., the ability of the group or person to acquire, weaponize, and deliver a specific pathogen or toxin in quantities sufficient to cause mass casualties.
 - The attributes of pathogens or toxins of possible utility to terrorists, including, if a pathogen, its infectivity, virulence, effective dose, hardiness, ease of production, and handling safety for operators or, if a toxin, its toxicity, effective dose, ease of production, ease of dispersal, and half-life in the open environment.
 - The range of possible targets for bioterrorist attack, taking into account the group's intent and technical capabilities, as well as the characteristics of the environs where the attack is to take place and the vulnerabilities of the target population.
2. Associated with each threat are potential outcomes, including cost consequences, which may be prevented or reduced in severity by using different defensive strategies (risk management). Thus, the threat, if realized, will have a particular outcome, such as an epidemic causing illness among the target population, including a certain proportion of fatalities; and the outcome will have direct and indirect cost consequences, including outlay for direct health care costs, crowd control, and loss of work. Of course, there also will be costs related to developing and implementing preventive and emergency management strategies. However, such strategies, if well developed and implemented, can be expected to more than pay for themselves for three reasons: (1) if a community were to be spared a bioterrorist attack because preventive strategies worked, the enormous cost related to addressing the consequences of a bioterrorist attack would not have to be paid; (2) if a community were to be attacked, one can expect that adequate preparedness would lead to that community having fewer casualties than if there were

inadequate or no preparedness plans; and (3) there are subjective benefits associated with planning, such as the peace of mind enjoyed by a population safeguarded from a bioterrorist attack and having the knowledge that its public health system has been enhanced.

Workshop participants realized that a robust risk assessment of bioterrorism will require knowing more about individual or group motivations to commit terrorist acts, as well as the technical capabilities of groups or individuals who might wish to carry out such acts. Until such information becomes available, any efforts to either model a bioterrorist event or perform a risk assessment of bioterrorism will rely, out of necessity, heavily on expert judgments and assumptions. When these are used to bridge temporary data gaps, sensitivity analysis must be conscientiously employed so that their influence on a risk assessment's conclusions is clearly understood.

In conclusion, while recognizing that many challenges lay in the path of applying risk analysis techniques to bioterrorism, it was the consensus of the participants that developing such techniques would be very useful in designing a U.S. bioterrorism risk management strategy, and that such a strategy is worth pursuing. It was generally agreed that a program to develop such techniques would have to be undertaken by a multidisciplinary group of risk assessment experts, and that it probably would be an expensive and time-consuming exercise. In addition, the majority of workshop participants expressed a strong willingness to contribute their professional expertise to assist the U.S. government in dealing with the threat posed by bioterrorism. Further discussions among leading experts from the decision, risk analysis, and bioterrorism communities would seem an obvious and important need for planning how to develop needed threat assessment capabilities to improve the U.S. capabilities to protect against bioterrorism.

Raymond A. Zilinskas
Rapporteur
June 24, 2003

Discussion of Workshop Findings and Their Possible Implications

by

Raymond A. Zilinskas, Bruce Hope, and Warner North

June 24, 2003

The workshop was an opportunity for threat analysts from the defense establishment and intelligence community to interact with risk assessment experts from various disciplines who usually are not involved in security matters (and who had no specialized knowledge of terrorism). Workshop organizers hoped that through this interaction both sides would learn from one another and, using the newfound knowledge, propose new ideas or concepts for improved approaches to risk assessment of bioterrorism.

We found that regardless of the practical or scientific discipline in which an analyst was grounded, the workshop's consensus was that a quantitative risk assessment in that discipline depends on there being some reliable data available to the analyst. This is understandable given that risk assessments for human health, the environment, engineering, and other disciplines have become increasingly quantitative and typically are based on models, parameterized with empirical data of varying extent and quality. Thus, a quantitative bioterrorism risk assessment would need data or well-informed judgments on the intent of terrorist groups or individuals, their technical capabilities, the attributes of pathogens or toxins that might be used in a biological attack, target characteristics, and the occurrence (frequency) of various attack scenarios. While data regarding target and bioagent characteristics are available, to a lesser or greater extent, data on bioterrorist intent and the frequency of different types of attacks are nearly non-existent.

This data gap apparently stems from the rarity of bioterrorist events. To illustrate, a search of the Center for Nonproliferation Studies (CNS) Weapons of Mass Destruction (WMD) Terrorism database, which is the largest unclassified one of its kind, revealed that out of 383 incidents in which biological, chemical, nuclear, or radiological agents were used by criminals or terrorists during the time frame 1900 to the present (see Figure 1), only 77 biological "events" (i.e., episodes involving the deliberate use of a biological agent to harm people) were perpetrated (all figures and tables are located at the end of this draft report). Of these, just four post-1945 events generated more than ten casualties (Table 1). In addition, due to the unique characteristics of each known biological attack, there does not appear to be a consistent pattern that could be used to predict the frequency of other bioterrorist or biocriminal events. This data deficit poses three challenges for the risk analyst:

- the small number of cases makes it difficult to develop a strong prediction methodology; i.e., one that would reliably assess the likelihood of future attacks. Large uncertainties will remain. Assumptions and judgments, rather than statistical data, must provide the basis for such assessments.
- the likely low rate of future attacks involving pathogens also makes it very difficult to calibrate, much less validate, whatever predictive methodology that might be developed.
- information on intent and capabilities of terrorist groups or individuals who aim to mount biological attacks is extremely difficult to obtain. It is possible, but unclear at this point, that additional intelligence efforts will improve this situation.

The difficulties with developing predictive methodology are illustrated by the events of September and October 2001. Over a period of approximately one month, five envelopes containing *Bacillus anthracis* spores were mailed to various public figures. Eventually, 22 persons contracted cutaneous or inhalation anthrax, of whom five died. In addition, these biological letter bombs caused billions of dollars to be spent by the U.S. government for new security measures and environmental remediation. While it may have been possible to anticipate the probability of this mode of attack, including the pathogen most suitable for this purpose (Brown 2002), it appears that neither the targets of attack, nor the person or group responsible for attacks, could have been predetermined by any known threat assessment methodology. What might have been predicted was that the U.S. mail system could not only be used as a means to deliver anthrax, but also that a letter containing anthrax spores could spread spores among mail workers and to other recipients of mail besides the intended victims, through transfer of spores from the original letter to other pieces of mail (Griffith et al. 2003). It should not have been hard to predict that weaponized anthrax spores could escape from an envelope and spread by contact or aerosol. This prediction arises from the physics of particle size, the lack of tight seals on paper envelopes, and the kinds of pressure changes known to occur in envelopes going through mail sorting machines. Such a prediction might have permitted earlier actions to isolate and clean mail-handling facilities and to diagnose and treat those infected. Likewise, it is relatively obvious that a jet plane with nearly full fuel tanks can deliver a mammoth explosive force to a structure. This obvious insight, combined with an intelligence assessment that some terrorists might be willing to carry out suicide bombings, could have suggested that pre-September 11, 2001, guidance for airline pilots, crew, and passengers (i.e., to obey the instructions of hijackers) would be ineffective in averting a catastrophic outcome.

In view of the problems revealed by workshop proceedings and taking into account the shortcomings of previous attempts to assess risks pertaining to terrorism, what can be done in regards to both improve threat assessments and develop risk assessment methods for bioterrorism? We present three recommendations for consideration by the U.S. government, in particular the Department of Homeland Security; two for the short term and one for the longer term. Note that these recommendations are informed by both the November 2001 workshop and a subsequent meeting of some of the workshop participants at Lawrence Livermore National Laboratory in March 2003.

(1) Short-term: Threat Assessment Methodologies

When some information is available that characterizes the potential assailant and gives clues as to the means likely to be used to carry out an attack, an analyst may apply existing threat assessment methodologies to assess a specific threat.

An expressed threat, whether explicit or implied, can be evaluated using methodology developed by the security-provider industry and public protective agencies. This is possible because, over the years, data have been collected from incidents when they or their clients were threatened with violence, and where some threats were realized but most were not. By putting together data derived from content analysis of the threatening statement, an assailant's history, and interviews of persons who are or were acquainted with the assailant, sufficient information can be collected for a fairly robust assessment of the threat that assailant presents to society in general or to a particular target. A methodology to accomplish a threat analysis with this level of data availability has been developed by, for example, the U.S. Secret Service and Gavin de Becker and Associates (Committee on Research and Training Issues Related to the Mission of

the Secret Service 1984; Fein & Vossekuil 1998; de Becker 2002). This methodology, which is probably known to government security personnel generally, would be applicable if an explicit written or verbal threat were to be issued against a facility or population by an individual or group that could be identified and investigated.

It is important to note, however, that none of the past known biological or other terrorist attacks that caused mass casualties were preceded by the issuance of any warning (Hansen 2002). Therefore, if the past is a guide, it is highly unlikely that future threats to facilities or populations from criminals or terrorists wielding biological weapons will be known to or recognized by security personnel until after they are realized.

(2) Short-term: Vulnerability Analysis

To perform a quantitative risk assessment of bioterrorism, the analyst would require some data on various aspects of the problem, including (but not limited to): a terrorist group's willingness to use a weapon of mass destruction; a terrorist group's technical capability to acquire and deploy a biological weapon; the target population or facility that a terrorist group would be likely to attack; the pathogens or toxins that are most accessible to the terrorist group; the characteristics and quantity of the pathogen or toxin formulation that would arm the biological weapon; the weapon deployment scenario (e.g., point source or line source); and, for line-source aerosol dispersal, the meteorological conditions at the time of dispersal, or for point-source dispersal (e.g., foodborne or beverage-borne), the characteristics of the food or beverage to be contaminated. If this data were available, it would be possible for the analyst to identify the hazard, calculate the dose-response, estimate exposure and, thus, determine not only the probability of the target population suffering adverse effects, but also its likely number of casualties. Such data are likely, however, to be difficult to obtain or may not exist at all. This paucity of data suggests that a bioterrorism risk assessment would need to occur in two stages (Figure 2): a qualitative or semi-qualitative *vulnerability analysis* stage, followed, depending on data availability, by a more quantitative *risk estimation* stage, with the latter involving four components: hazard characterization, hazard identification, exposure assessment, and risk characterization (Figure 3).

For the short term, the U.S., including federal, state and local perspectives, may simply assume that bioterrorist attacks on its assets (personnel, facilities, infrastructure, and activities) are possible and perform vulnerability studies to develop preparedness and response plans. As a writer has stated in a similar context, "When scientific knowledge about probabilities is absent, thinking about possible outcomes takes on a particular significance" (Anand 2002). A vulnerability analysis seeks to identify a valuable asset (i.e., a target) at risk of a bioterrorist attack and to conceptualize various ways in which it is vulnerable to such an attack (i.e., various attack scenarios). It starts by clearly stating the assessment's scale and scope (e.g., the world, a country, a specific facility?), with the understanding that the risk assessment problem becomes increasingly more tractable as the scope narrows. Since human, animal, or plant populations could be attacked with biologicals in a large number of ways, some might say that the number of potential attack scenarios could be very high, possibly to the point of analytical paralysis. This might be so if our society as a whole would be considered as a target, but not so if the focus is substantially narrowed to something specific, such as a defined population or discrete facility. If this is done, risk analysts should be able to construct plausible and credible attack scenarios applicable to that particular situation.

The analysis would then use currently available technical and intelligence information, along with expert elicitation and best professional judgment to, in the first instance, conceptualize combinations of targets (i.e., valued assets deemed important to protect), bioagents, exposure pathways (i.e., how a bioagent could reach the target), and potential adverse outcomes into "attack scenarios". This process may also be referred to as logic modeling, problem formulation, or conceptual modeling (United States Environmental Protection Agency 1998). Available information might include: pathogens or toxins that might be used to harm the target area's population and/or contaminate its environment, methods that might be used to disperse pathogens or toxins to achieve attack objectives, and the means attackers would use to emplace mechanisms for dispersing pathogens or toxins so as to have the highest probability of harming the facility's population and contaminating its environs. For our purpose, "adverse outcomes" could be defined, for example, as "using a biological weapon is such a way as to generate mass casualties among a target population," or "using a biological weapon in such a way as to cause a sufficient level of panic in a target population so its social and political structure dissolves." These scenarios then could be comparatively ranked based on their probability of occurrence and nature and magnitude of consequences should they occur. Such a comparative ranking may, in and of itself, be sufficient to focus and support risk management decision-making. The vulnerability analysis process should permit analysts to concentrate their efforts on attack scenarios revealing weaknesses that in fact could be recognized and exploited by terrorists, while avoiding undue analysis of scenarios that would not or could not be used. Such focused vulnerability studies; i.e., those that concentrate on a target important to, for example, a government agency, and which for that reason must be protected from a biological attack, probably is the best method for designing defenses for vulnerable, important targets.

Several concepts and definitions useful to the performance of a vulnerability study may be presented (Martz & Johnson 1987):

- Static target – a target whose vulnerability is constant over time so the threat level also is constant. The population of a metropolitan area can be considered static, although individuals of that population on a continuous basis will be moving in and out of the facility under consideration.
- Dynamic target – a target whose vulnerability changes with time. There are two types of dynamic targets – a moving target and a static target with varying exposure. A moving target could be a train or truck carrying cargo or supplies from one location to another or from a supplier to the consumer. An example of a static target with varying exposure is the population of commuters using a subway system.
- A dynamic operation can be divided into a set of non-overlapping time intervals, where an "interval" is defined as a period of time in which the perceived threat level is relatively constant. There may or may not be spatial movement of the target during a given interval and the safeguards may be different for different intervals. However, when dealing with a biological attack, many factors can affect the "perceived threat level." For example, the perceived threat level can be affected by a static target having varying vulnerability. Thus, if we were concerned about a typical workplace facility, the likelihood of it suffering a biological attack could be perceived to be low during the interval of a weekend (when most of the workforce is absent), but relatively higher during the interval

of the workweek. Similarly, a biological attack would be unlikely during a time interval as defined by a rain or snow storm.

Hope (2001) has developed scenarios for biological attacks against agricultural and food industry targets by viewing the food supply system as “a set of interconnected nodes...and each node is assumed to have the some logical structure (although with potentially different parameter values).” This approach could be used to identify a system’s or facility’s components, as well as connections between these components, and analyze each component and connection for vulnerabilities to biological intrusion, taking into account the concept of time intervals as suggested by Martz and Johnson (1987). If this was done, we estimate that a majority of plausible biological attack scenarios faced by a system or facility could be identified, allowing the major ones (those of highest probability and greatest consequence) to be addressed by deploying countermeasures. It is probable that many facilities and, possibly, some populations could immediately be eliminated from being considered as targets to biological attacks either permanently (e.g. bridges and railroads) and others at certain times (e.g. open stadiums when rain or snow is falling or workplaces that are empty on holidays).

It is further probable that many structures could be secured relatively easily from major biological attacks. For example, an office building, wherever located, is likely to have just five entry points to terrorists wielding biological weapons; the air-handling system, the food-handling system (if present), the water delivery system, the mail delivery system, and the personnel and visitor entry system. Defensive measures at just these five entry points could render that building invulnerable, or nearly so, to a bioterrorist attack, substantially more so than a similar office building without such controls. Of course, a determined adversary could still attempt to breach the protected building’s defenses by, for example, breaking through the grill protecting an air intake conduit or injecting pathogens into the main delivering water to the building, but it would take much more effort to mount a successful attack, the chance of detection while attempting to gain entry would be higher, and the overall probability of these attack scenarios being successfully carried out would be lower. So, would the terrorist not instead select an attack scenario with a higher probability of success?

The foregoing are examples of how vulnerability studies of facilities or locations might be carried out, and should be sufficient to demonstrate that such studies could be done in a meaningful way; e.g., they would produce findings useful to managers who seek to put into place defenses that would defeat biological attacks on important assets. However, since there are many potential attack scenarios, and since terrorists have proven adapt at exploiting new ones as old ones are defended against, there will be an on-going need to enhance existing vulnerability study methodologies to take advantage of applications from scientific and technical advances so as to continue to generate actionable findings of use to managers.

(3) Longer-term: Quantitative Risk Assessment & Modeling

For a longer-term project, we suggest augmentation and enhancement of vulnerability studies through the application of quantitative (and probabilistic) risk estimation techniques, supported by use of modeling exercises. Developing a quantitative risk estimate for a bioterrorist attack presupposes that a vulnerability analysis, to narrow the scope and identify attack scenarios worthy of more detailed analysis, has occurred. Risk estimation then gathers what quantitative data are available regarding the attack scenario and proceeds through four steps - hazard characterization, hazard identification, exposure assessment, and risk characterization (Figure 3)

- to provide a numeric estimate of the risk posed by that scenario (National Research Council, 1983, 1996, 2002 [see especially Chapter 10 in the last report]). Risk estimation generally involves development of a model or models. Human health and environmental risk assessments have become increasingly quantitative and are typically based on models, parameterized with empirical data of varying extent and quality (North et al. 1975; Taylor et al., 1998; Leonard 2001; Kunreuther 2002). Data can also be obtained through expert elicitation, by appeals to best professional judgment, and by assuming a bounding range of possible values - rarely is there absolutely no data for risk estimation (Zilinskas 1998; MacGregor and Race 2001; Kass 2002). Pathogen risks to humans, crops, and livestock have been estimated with a variety of models; for example: quantitative dose-response (United States Department of Agriculture 1998; Coleman and Marks 1999), fault tree (Marks *et al.* 1998), and epidemiological (Pybus *et al.*, 2001). Similar models have been applied to political terrorism (Koller 2000, Zanders et al. 2000) and suggested for application to anti-crop bioterrorism (Madden and Scherm 1999). From these studies we deduce that risk estimation typically is an iterative process. Information gained in each step is combined to represent a cause-and-effect chain, from the prevalence and concentration of an intentionally introduced bioagent to the probability and magnitude of adverse outcomes in the valued asset being targeted.

Modeling can be used to produce a representation or simulation of a biological attack. Modeling of possible untoward events, including biological events, has, of course, been done for many years by security experts. Modeling was done as part of the pre-1969 U.S. offensive biological warfare program to assess possible biological attacks on cities, airports, subway systems, and other targets. These models should be reviewed by today's security experts as to their applicability to the present threat environment and upgraded if determined to still be useful. If, however, these older models prove to be largely inappropriate or inadequate, then new models should be designed, taking into consideration the current concern about terrorists of both international and domestic origin. Activities to do this are already proceeding (Berawal & Merkle 2001).

To visualize the role of modeling in the risk estimation process, consider this hypothetical scenario: a vulnerability analysis (see section 2) of Facility A concludes that, due to prevalent meteorological conditions and the proximity of an unrestricted road, it is vulnerable to aerosol attack. A model would then simulate various agent formulations (e.g., those containing a viral species, a bacterial species, and a toxin) being released as a spray from a passing truck. Assuming meteorological conditions conducive to an aerosol attack, the model would provide data on how efficiently each formulation would be transported and dispersed, as well as the likely fate of the agents in the various formulations (i.e., their survivability or persistence in the open environment). With this data, the risk analyst could estimate doses to which facility workers would be exposed, the probable adverse outcomes in workers at these doses, and characterize the risk posed to workers by each formulation. With risk assessment results in hand, facility managers could then determine the types of defensive measures that would have to be taken to eliminate or mitigate the consequences of this particular attack scenario.

At the early stage of development, the goal would not, indeed could not, be a reliable predictive risk model (any such models for bioterrorism can initially be expected to be crude), but rather a framework within which to accommodate the breadth of available information about a particular scenario or bioagent. Such models would, however, be constantly updated and improved as each new related study and intelligence update provides additional relevant data. Placing all of the information in one, consistent framework allows for clearer delineation of gaps

in knowledge, provides a focus for discussions among workers from diverse disciplines, and best describes what is currently known and unknown. It also can provide a sound basis for cost-benefit analysis of proposed research or specific intelligence gathering efforts. Such models support decision making not only by providing a risk estimate for a given scenario but also by allowing decision makers to test assumptions and perform "what if" analyses on alternative countermeasures for reducing or eliminating credible threats, as well as to consider and compare countermeasure strategies that would be very difficult to test in a "live" environment (Government Accounting Office 1998).

In conclusion, in the future our society is likely to experience more bioterrorist attacks. If so, each would generate information that is applicable to subsequent, ever improving, risk assessments. If, however, bioterrorist attacks remain very rare occurrences, and their characteristics differ significantly, then our ability to perform quantitative risk assessments will continue to be hampered by a lack of empirical data. If this is so, we must improve the ability of defenders to perform vulnerability analyses and use the information generated by these analyses to develop better defenses. To the extent practicable, quantitative risk estimation should be attempted on those attack scenarios deemed high probability and high consequence by vulnerability analysis, using expert elicitation and probabilistic techniques to bridge data gaps. Such attempts will provide valuable insight into what changes are necessary to make risk assessment a useful tool for the management of bioterrorist threats.

References

- Anand, P. 2002. Decision-making when science is ambiguous. *Science* 295:1839.
- Beriwal, M. & Merkle, P.B. 2001. *Defense Threat Reduction Agency CB Modeling and Simulation Futures Workshop*, Advanced Systems and Concepts Office, Defense Threat Reduction Agency, Washington, D.C.
- Broad, W.J. 2001. Experts call for better assessment of threats. *New York Times*, October 2, p. 1.
- Brown, D. 2002. Agency with most need didn't get anthrax data: CDC unaware of Canadian study before attacks. *Washington Post*, February 11, p. A3.
- Coleman, M.E. & Marks, H.M. 1999. Qualitative and quantitative risk assessment. *Food Control* 10:289-297.
- Committee on Research and Training Issues Related to the Mission of the Secret Service. 1984. *Research and Training for the Secret Service: Behavioral Science and Mental Health Perspectives*, National Academy Press, Washington, D.C.
- de Becker, Gavin. 2002. *Mosaic Threat Assessment Systems*. Gavin de Becker and Associates, Los Angeles, CA (restricted circulation).
- Fein, R.A. & Vossekuil, B. 1998. *Protective Intelligence & Threat Assessment Investigations*, National Institute of Justice, U.S. Department of Justice, Washington, D.C., NCJ 170612.
- Government Accounting Office. 1998. *Combating Terrorism: Threat and Risk Assessments Can Help Prioritize and Target Program Investments*. GAO/NSIAD-98-74. Government Accounting Office, National Security and International Affairs Division, Washington, D.C.
- Government Accounting Office. 1999. *Combating Terrorism: Need for Comprehensive Threat and Risk Assessment of Chemical and Biological Attacks*. GAO/NSIAD-99-163. Government Accounting Office, Washington, D.C.
- Griffith, Kevin S. et al. 2003. Bioterrorism-related inhalational anthrax in an elderly woman, Connecticut, 2001. *Emerging Infectious Diseases* 9(6):681-688.
- Hansen, S. 2002. America's homegrown terrorists: An expert on right-wing hate groups talks about the tortured emotional roots of their rage, their response to Sept. 11 and their role in the Oklahoma City bombing. Salon.com, January 17.
- Homsy, Robert V. & Zilinskas, Raymond A. 2001. Background Paper: Bioterrorism Threat Assessment and Risk Management Workshop, held at the Monterey Institute of International Studies, Washington, D.C., November 12-13.

- Hope, Bruce K. 2001. A Risk Assessment Perspective on Bioterrorist Threats to the U.S. Food Supply. September 27 (submitted to *Human Health and Ecological Risk Assessment*).
- Kass, L. 2002. Threat assessment methodology. Personal communication of March 15.
- Koller, G.R. 2000. Terrorism risk models – Relative and absolute risk. In *Risk Modeling for Determining Value and Decision Making*. Chapman & Hall/CRC Press, Washington, D.C., pp. 21-65.
- Kunreuther, H. 2002. Risk analysis in an uncertain world. *Risk Analysis* 22(4): 655-664.
- Leonard, A. 2001. Outlook bright for catastrophe modeling. *Reinsurance Magazine*, October 7.
- MacGregor, D.G. & Race, M.S. 2001. Microbiologists' Perception of Planetary Protection. Unpublished Work.
- Madden, L.V. & Scherm, H. 1999. Epidemiology and risk assessment. A symposium on *Plant Pathology's Role in Anti-Crop Bioterrorism and Food Security*. Joint American and Canadian Phytopathological Society meeting, Montreal, Canada, August 7-11.
- Marks, H.M., Coleman, M.E., Lin, C-T.J., & Roberts, T. 1998. Topics in microbial risk assessment: Dynamic flow tree analysis. *Risk Analysis* 18:309-328.
- Martz, H.F. & Johnson, M.E. 1987. Risk analysis of terrorist attack. *Risk Analysis* 7(1):35-47.
- National Research Council. 1983. *Risk Assessment in the Federal Government: Managing the Process*, National Academy Press, Washington, D.C.
- National Research Council, 1996. *Understanding Risk: Informing Decisions in a Democratic Society*, National Academy Press, Washington, D.C.
- National Research Council, 2002. *Making the Nation Safer: The Role of Science and Technology in Countering Terrorism*, National Academy Press, Washington, D.C.
- North, D.W., Judd, B.R., & Pezier, J.P. 1975. New methodology for assessing the probability of contaminating Mars, in *Life Sciences and Space Research XIII. Proceedings of the Open Meeting of the Working Group on Space Biology of the Seventeenth Plenary Meeting of COSPAR*, P.H.A. Sneath (ed.), Akademie-Verlag, Berlin, pp. 103-109.
- Office of the Inspector General. 2002. *A Review of the Federal Bureau of Investigation's Counterterrorism Program: Threat Assessment, Strategic Planning, and Resource Management*, Report No. 02-38; ><http://www.usdoj.gov/oig/audit/0238/exec.htm><.
- Palarino, R.N. 2001. *Media Advisory: Briefing memorandum for the hearing Combating Terrorism: Assessing the Threat of Biological Terrorism, scheduled for Friday October 12, 2001, at 10:00 AM in room 2154 Rayburn House Office Building*, Subcommittee on National

Security, Veterans Affairs, and International Relations, House of Representatives, Washington, D.C.

Pybus, O.G., Charleston, M.A., Gupta, S., Rambaut, A., Holmes, E.C., & Harvey, P.H. 2001. The epidemic behavior of the hepatitis C virus. *Science* 292: 2323-2325.

Taylor, C., Vanmarcke, E., & Davis, J. 1998. Evaluating models of risks from natural hazards, in *Paying the Price: The Status and Role of Insurance Against Natural Disasters in the United States*, National Academy Press, Washington, D.C., pp. 239-249.

United States Department of Agriculture. 1998. *Salmonella enteritidis Risk Assessment Shell Eggs and Egg Products, Final Report*. Food Safety and Inspection Service, U.S. Department of Agriculture, Washington, D.C.

United States Environmental Protection Agency. 1998. *Guidelines for Ecological Risk Assessment, Final*. EPA/630/R-95/002F. Risk Assessment Forum, U.S. Environmental Protection Agency, Washington, D.C.

Zanders, Jean P. et al. 2000. Risk assessment of terrorism with chemical and biological weapons, in *SIPRI Yearbook 2000. Armaments, Disarmament and International Security*, Stockholm International Peace Research Institute (ed.), Oxford University Press, New York, pp. 537-559.

Zilinskas, Raymond A. 1998. Analysis of the ecological risks associated with genetically engineered marine microorganisms, in *Genetically Engineered Marine Organisms: Environmental and Economic Risks and Benefits*, Raymond A. Zilinskas & Peter J. Balint, eds., Kluwer Academic Publishers, New York, pp. 95-138.

Table 1: BIORCRIMINALITY 1945-2002

- 1. Mitsuru Suzuki, 1964-1966 (foodborne – 64 victims/0 deaths);**
- 2. The Rajneeshees, 1984 (foodborne – 751 victims/0 deaths);**
- 3. Diane Thompson, 1996 (foodborne – 12 victims/0 deaths);**
- 4. Unknown, September/October 2001 (aerosol – 22 victims/5 deaths).**

Table 2: Technical and Operational Disciplines and Relevant Questions

Intelligence integration and source term	What is the quantitative nature of the event(s) initiating the chemical-biological hazard condition? How much can be known prior to release, during an event, on in forensic reconstruction of a release event?
Transport, dispersion, fate, and terrain	What happens to the agent after release, through dilution, transformation, deposition, re-suspension, and terrain-related processes?
Weather (atmospheric dynamics)	Weather prediction and data acquisition can provide data on meteorological phenomena playing central roles in hazard evolution. How could this discipline more fully enable chemical-biological hazard prediction?
Dose-response	How are humans, animals, and plants affected by a given exposure to agents?
Population epidemiology	How do effects of chemical-biological agent releases propagate and persist in exposed populations?
Agriculture and biota	What are the strategic defense issues and the role of the DoD M&S program, in view of the potential for both accidental and deliberate introductions of chemical-biological agents?
Materiel	The impact of chemical-biological agents on defense materiel, transport, and support systems could be significant. Do we understand the key uncertainties in this area?

Figure 1

(Source: Monterey WMD Terrorism Database)

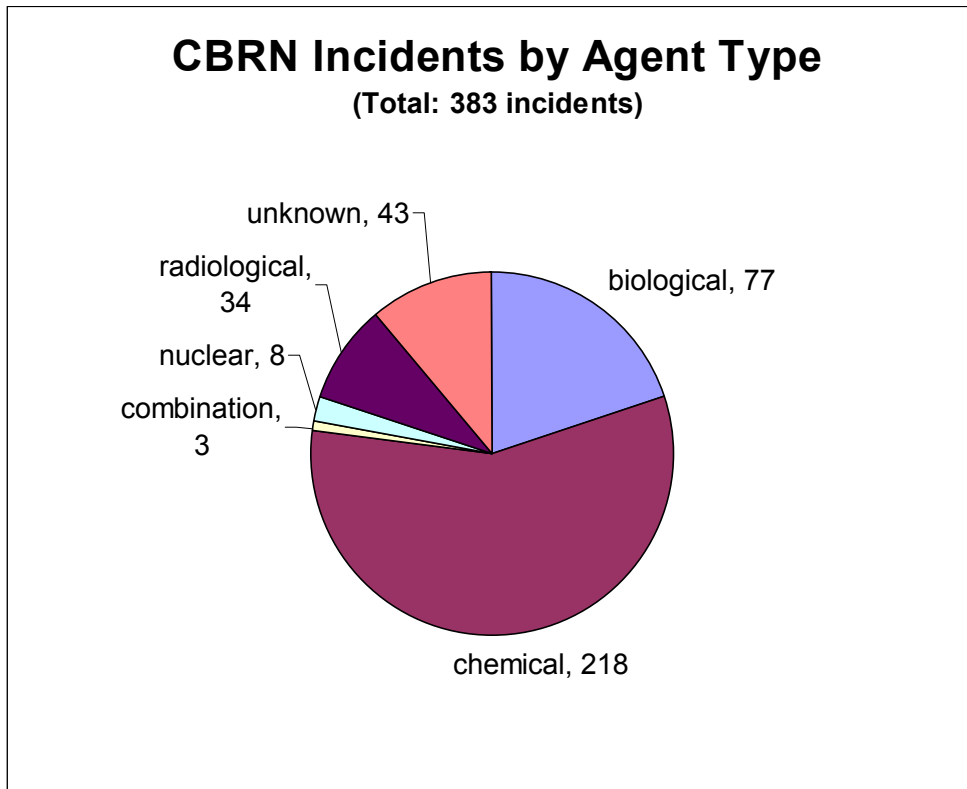


Figure 2

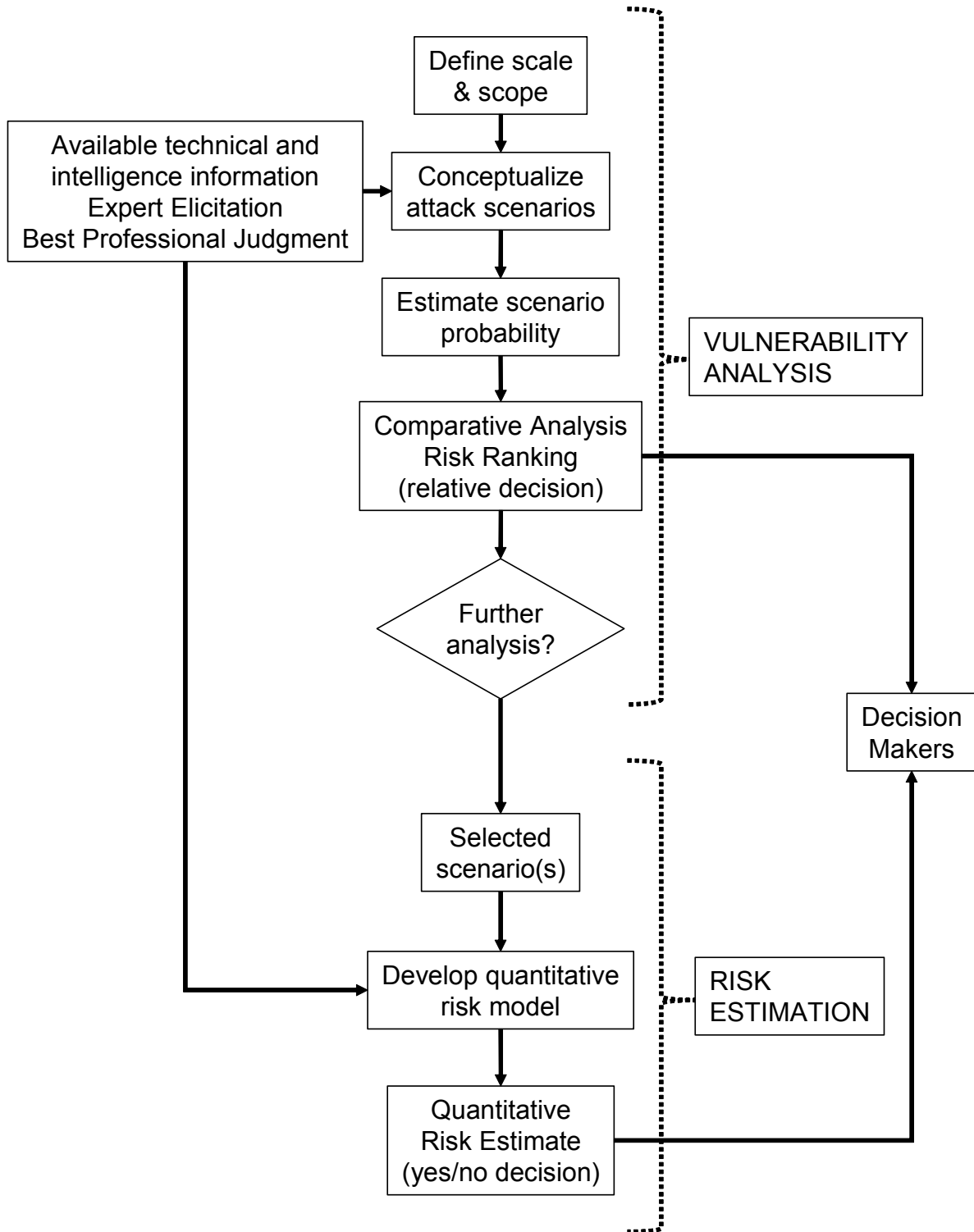
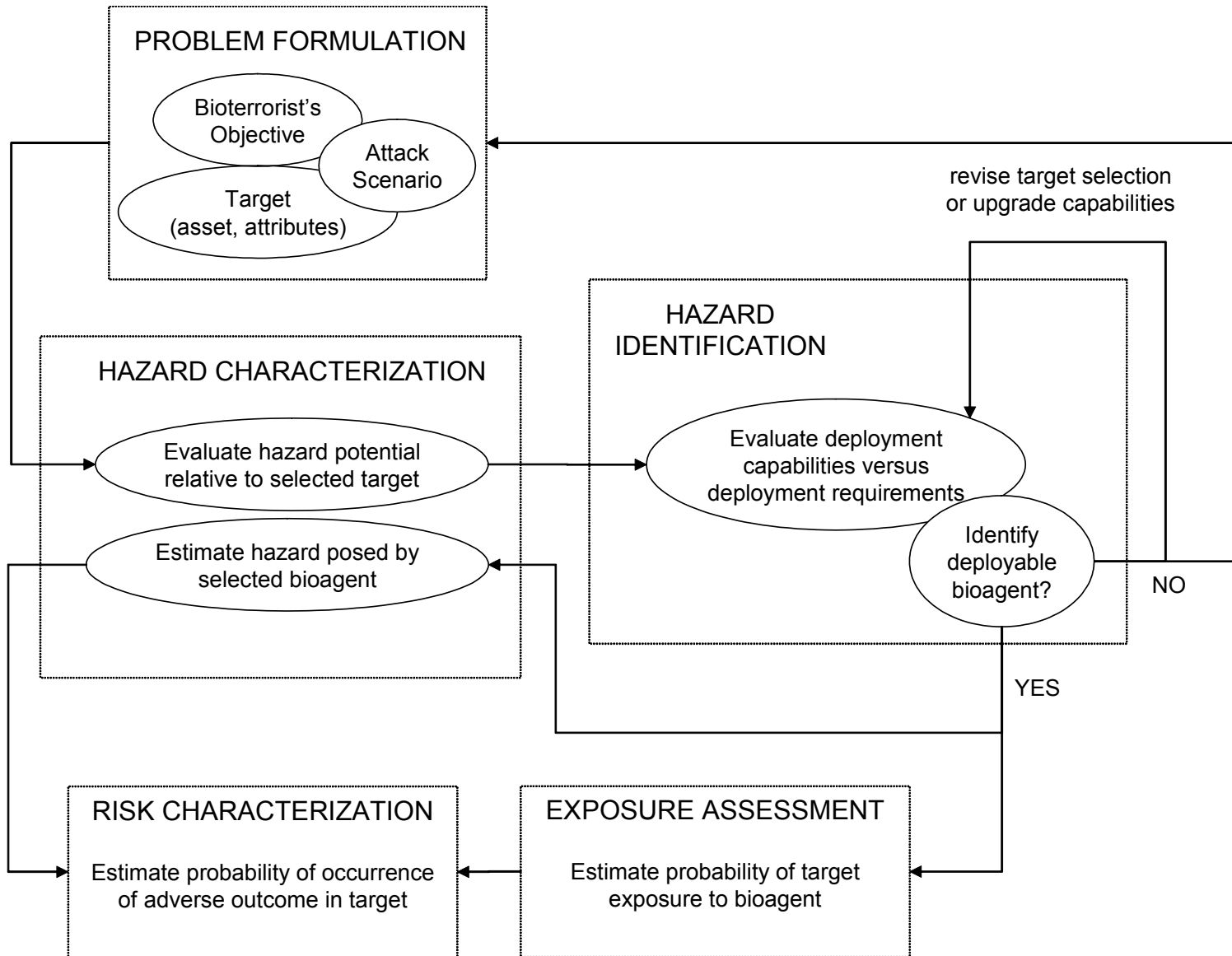


Figure 3



Annex 1: List of Workshop Participants

Pete L. Estacio M.D.
Lawrence Livermore National Laboratory
Livermore, CA

Steve Fogarty
Risk Applications Development
ARES Corporation
Albuquerque, NM

David R. Franz, DVM, Ph.D.
Chemical & Biological Defense Division
Southern Research Institute
Frederick, MD

Julie Fruetel, Ph.D.
Sandia National Laboratory
Livermore, CA

John Garrick, Ph.D., P.E.
PLG, Inc.
Irvine, CA

Esin Gulari, Ph.D.
National Science Foundation
Washington, D.C.

Robert V. Homsy, Ph.D.
Lawrence Livermore National Laboratory
Livermore, CA

Bruce Hope, Ph.D.
Oregon Department of Environmental Quality
Portland, OR

Victor S. Koscheyev, M.D., Ph.D., Sc.D.
Laboratory for Health and Human Performance in Extreme Environments
University of Minnesota
Minneapolis, MN

Howard Kunreuther, Ph.D.
Wharton Risk Management and Decision Processes Center
University of Pennsylvania
Philadelphia, PA

Morris A. Levin, Ph.D.
University of Maryland Biotechnology Institute (emeritus)
College Park, MD

William C Maier, Ph.D., MPH
Respiratory and Psychiatry Epidemiology
GlaxoSmithKline Company
Greenford, Middlesex UB6 0HE, UK

Fred Milanovich, Ph.D.
Lawrence Livermore National Laboratory
Livermore, CA

D. Warner North, Ph.D.
NorthWorks, Inc.
Belmont, CA

Amy Sands, Ph.D.
Center for Nonproliferation Studies
Monterey Institute of International Studies
Monterey, CA

Paul Slovic, Ph.D.
Decision Research
Eugene, OR

Page Stoutland, Ph.D.
Lawrence Livermore National Laboratory
Livermore, CA

Jonathan B. Tucker, Ph.D.
Center for Nonproliferation Studies
Monterey Institute of International Studies
Washington, D.C.

Bryan S. Ware
Digital Sandbox, Inc.
Reston, VA

Richard Wheeler, Ph.D.
Lawrence Livermore National Laboratory
Livermore, CA

Alan P. Zelicoff, MD
Center for National Security and Arms Control
Sandia National Laboratories
Albuquerque, NM

Raymond A. Zilinskas, Ph.D.
Center for Nonproliferation Studies
Monterey Institute of International Studies
Monterey, CA

Annex 2: Participants of the March 27, 2003, Meeting in Livermore, CA

Dr. Bruce Hope

Dr. Howard Kunreuther (by telephone)

Dr. Warner North

Mr. Bryan Ware (by telephone)

Dr. Richard Wheeler

Dr. Raymond A. Zilinskas