Interim Report on Methodological Improvements to the Department of Homeland Security's Biological Agent Risk Analysis

Committee on Methodological Improvements to the Department of Homeland Security's Biological Agent Risk Analysis, National Research Council

ISBN: 0-309-66957-X, 24 pages, 8 1/2 x 11, (2007)

Interim Report on Methodological Improvements to the Department of Homeland Security's Biological Agent Risk Analysis

Committee on Methodological Improvements to the
Department of Homeland Security's
Biological Agent Risk Analysis

Board on Mathematical Sciences and Their Applications

Division on Engineering and Physical Sciences

NATIONAL RESEARCH COUNCIL
OF THE NATIONAL ACADEMIES

THE NATIONAL ACADEMIES PRESS
Washington, D.C.
www.nap.edu

THE NATIONAL ACADEMIES PRESS 500 Fifth Street, N.W. Washington, DC 20001

NOTICE: The project that is the subject of this report was approved by the Governing Board of the National Research Council, whose members are drawn from the councils of the National Academy of Sciences, the National Academy of Engineering, and the Institute of Medicine. The members of the committee responsible for the report were chosen for their special competences and with regard for appropriate balance.

This study was supported by Contract No. HSHQDC-06-C-00046 between the National Academy of Sciences and the Department of Homeland Security. Any opinions, findings, conclusions, or recommendations expressed in this publication are those of the author(s) and do not necessarily reflect the views of the organizations or agencies that provided support for the project.

Additional copies of this report are available from the National Academies Press, 500 Fifth Street, N.W., Lockbox 285, Washington, DC 20055; (800) 624-6242 or (202) 334-3313 (in the Washington metropolitan area); Internet, http://www.nap.edu.

Printed in the United States of America

THE NATIONAL ACADEMIES

Advisers to the Nation on Science, Engineering, and Medicine

The **National Academy of Sciences** is a private, nonprofit, self-perpetuating society of distinguished scholars engaged in scientific and engineering research, dedicated to the furtherance of science and technology and to their use for the general welfare. Upon the authority of the charter granted to it by the Congress in 1863, the Academy has a mandate that requires it to advise the federal government on scientific and technical matters. Dr. Ralph J. Cicerone is president of the National Academy of Sciences.

The **National Academy of Engineering** was established in 1964, under the charter of the National Academy of Sciences, as a parallel organization of outstanding engineers. It is autonomous in its administration and in the selection of its members, sharing with the National Academy of Sciences the responsibility for advising the federal government. The National Academy of Engineering also sponsors engineering programs aimed at meeting national needs, encourages education and research, and recognizes the superior achievements of engineers. Dr. Wm. A.Wulf is president of the National Academy of Engineering.

The **Institute of Medicine** was established in 1970 by the National Academy of Sciences to secure the services of eminent members of appropriate professions in the examination of policy matters pertaining to the health of the public. The Institute acts under the responsibility given to the National Academy of Sciences by its congressional charter to be an adviser to the federal government and, upon its own initiative, to identify issues of medical care, research, and education. Dr. Harvey V. Fineberg is president of the Institute of Medicine.

The **National Research Council** was organized by the National Academy of Sciences in 1916 to associate the broad community of science and technology with the Academy's purposes of furthering knowledge and advising the federal government. Functioning in accordance with general policies determined by the Academy, the Council has become the principal operating agency of both the National Academy of Sciences and the National Academy of Engineering in providing services to the government, the public, and the scientific and engineering communities. The Council is administered jointly by both Academies and the Institute of Medicine. Dr. Ralph J. Cicerone and Dr. Wm. A. Wulf are chair and vice chair, respectively, of the National Research Council.

www.national-academies.org

COMMITTEE ON METHODOLOGICAL IMPROVEMENTS TO THE DEPARTMENT OF HOMELAND SECURITY'S BIOLOGICAL AGENT RISK ANALYSIS

GREGORY S. PARNELL, U.S. Military Academy, *Chair*
DAVID BANKS, Duke University
LUCIANA BORIO, University of Pittsburgh
GERALD BROWN, Naval Postgraduate School
L. ANTHONY COX, JR., Cox Associates
JOHN GANNON, BAE Systems
ERIC HARVILL, Pennsylvania State University
HOWARD KUNREUTHER, University of Pennsylvania
STEPHEN MORSE, Columbia University
MARGUERITE PAPPAIOANOU, University of Minnesota
STEPHEN POLLOCK, University of Michigan
NOZER SINGPURWALLA, George Washington University
ALYSON WILSON, Los Alamos National Laboratory

Staff

SCOTT WEIDMAN, Director, Board on Mathematical Sciences and Their Applications
NEAL GLASSMAN, Senior Staff Officer, Board on Mathematical Sciences and Their Applications
KERRY BRENNER, Senior Staff Officer, Board on Life Sciences
BARBARA WRIGHT, Administrative Assistant

BOARD ON MATHEMATICAL SCIENCES AND THEIR APPLICATIONS

For more information on BMSA, see its Web site at http://www7.nationalacademies.org/bms/, write to BMSA, National Research Council, 500 Fifth Street, N.W., Washington, DC 20001, call (202) 334-2421, or send e-mail to bms@nas.edu.

Acknowledgments

This report has been reviewed in draft form by individuals chosen for their diverse perspectives and technical expertise, in accordance with procedures approved by the National Research Council's Report Review Committee. The purpose of this independent review is to provide candid and critical comments that will assist the institution in making its published report as sound as possible and to ensure that the report meets institutional standards for objectivity, evidence, and responsiveness to the study charge. The review comments and draft manuscript remain confidential to protect the integrity of the deliberative process. We wish to thank the following individuals for their review of this report:

John Bailar III, University of Chicago,
Gerald Dinneen, Lexington, Massachusetts,
Randall Larsen, The Institute for Homeland Security,
Stephen Robinson, University of Wisconsin,
Harvey Rubin, University of Pennsylvania, and
Lawrence Wein, Stanford University.

Although the reviewers listed above have provided many constructive comments and suggestions, they were not asked to endorse the conclusions or recommendations nor did they see the final draft of the report before its release. The review of this report was overseen by Frank Stillinger, Princeton University. Appointed by the National Research Council, he was responsible for making certain that an independent examination of this report was carried out in accordance with institutional procedures and that all review comments were carefully considered. Responsibility for the final content of this report rests entirely with the authoring committee and the institution.

The committee also acknowledges the valuable contribution of the following individuals, who provided input at the meeting on which this interim report is based:

James Petro, White House Homeland Security Council,
Adam Rose, Pennsylvania State University,
Detlof von Winterfeldt, University of Southern California, and
Staff of the Battelle Memorial Institute, Columbus, Ohio.

Contents

Executive Summary

In recognition of potential bioterrorist threats, President George W. Bush issued Homeland Security Presidential Directive 10 (HSPD10), “Biodefense for the 21st Century,” on April 28, 2004.[1] This directive, as well as the National Strategy for Homeland Security,[2] published by the White House Office of Homeland Security in 2002, required assessments of the biological weapons threat to the nation and assigned the Department of Homeland Security (DHS) responsibility for conducting these assessments, in coordination with other appropriate federal departments and agencies. The first DHS bioterrorism risk assessment was completed on January 31, 2006, and the report documenting the assessment was published on October 1, 2006.[3]

THE COMMITTEE’S PRELIMINARY ASSESSMENT

The National Research Council (NRC) was asked by DHS to carry out a study to recommend improvements to the methodology used for DHS’s first bioterrorism risk assessment. The NRC study will issue two reports: interim (this report), focused on near-term improvements that can begin in federal Fiscal Year 2007 (FY2007), and final, to recommend longer-term improvements.

On August 28-29, 2006, the NRC Committee on Methodological Improvements to the Department of Homeland Security’s Biological Agent Risk Analysis met with representatives of DHS, its National Biodefense Analysis and Countermeasures Center (NBACC), Battelle Memorial Institute, the White House Homeland Security Council, and the Homeland Security Center for Risk and Economic Analysis of Terrorism Events (CREATE). The briefings at this meeting described a probabilistic risk assessment (PRA) of 28 bioagents. For each of the 28 pathogens, it used a 17-step event-tree analysis of paths (sequences of events and actions) that could lead to the deliberate exposure of civilian populations. The recommendations and discussion below are based solely on those briefings; DHS’s bioterrorism risk assessment was not made available to the committee in time for this interim report.

This interim report provides DHS with overall near-term guidance and direction for the further development of its risk analysis models. The committee’s final report will address longer-term issues in the development of risk analysis capabilities for DHS. Because the topics discussed here will be studied in more depth and with a view toward the longer term, the committee’s final report will be more detailed and may modify the conclusions presented here. The committee is confident, however, that the recommendations included in this interim report are appropriate and necessary in the near term.

The committee recognizes that the development of this comprehensive suite of techniques used for the PRA is a logical extension of previous risk analysis methods used for natural and technological hazards and engineering design.[4] The implementation of the selected PRA framework appears, for the most part, to be consistent with well-accepted practice in other fields of risk analysis such as nuclear reactor safety and chemical safety. The committee also notes that DHS and its NBACC have sought ways to refine and improve this new capability.

[1] Homeland Security Presidential Directive 10, “Biodefense for the 21st Century,” April 28, 2004, available at http://www.fas.org/irp/offdocs/nspd/hspd-10.html. Accessed Nov. 1, 2006.
[2] See www.dhs.gov/xlibrary/assets/nat_strategy_hls.pdf. Accessed Nov. 1, 2006.
[3] *Bioterrorism Risk Assessment.* 2006. Biological Threat Characterization Center of the National Biodefense Analysis and Countermeasure Center. Washington, D.C.
[4] See, for instance, http://www7.nationalacademies.org/aseb/stamatelatos_nasa_presentation.pdf and http://www.ans.org/pubs/magazines/nn/docs/2000-3-2.pdf. Accessed Nov. 1, 2006.

THE COMMITTEE'S INTERIM RECOMMENDATIONS FOR FY2007

Based on its August 28-29, 2006, briefings, the committee's main concerns are about the overall purpose and directions of DHS's risk analysis, the challenges involved in structuring and predicting the actions of determined adversaries, and the need to provide policy makers with a sound foundation for DHS's ongoing risk analyses. Following are three critical interim recommendations.

Recommendation 1: DHS should establish a clear statement of the long-term purposes of its bioterrorism risk analysis.

A clear statement of the long-term purposes of the bioterrorism risk analysis is needed to enunciate how it can serve as a tool to inform risk assessment, risk perception, and especially risk-management decision making. Criteria and measures should be specified for assessing how well these purposes are achieved. Key issues to be addressed by such a statement should include the following: who the key stakeholders are; what their short- and long-term values, goals, and objectives are; how these values, goals, and objectives change over time; how the stakeholders perceive the risks; how they can communicate their concerns about these risks more effectively; and what they need from the risk assessment in order to make better (more effective, confident, rational, and defensible) resource-allocation decisions. Other important issues are who should perform the analyses (contractors, government, both) and how DHS should incorporate new information into the analyses so that its assessments are updated in a timely fashion.

Recommendation 2: DHS should improve its analysis of intelligent adversaries.

Event-tree methodology was not developed to model the possible actions of intelligent adversaries. Traditional event-probability assessment and elicitation techniques for these assessments are not sufficient for modeling the actions of intelligent adversaries made in response to their opponents' defensive actions and/or in response to initial successes or failures in their own plan execution. Alternative techniques—including red teams (i.e., individuals, including both technologists and those with experience in targeting and strategy, whose purpose is to simulate adversarial decision making) and attack-preference, decision-tree, attack-tree, or attack-graph models[5]—might be more suitable to complement elicitation.

Recommendation 3: DHS should increase its risk analysis methodology's emphasis on risk management.

It is unclear how the event-tree probabilistic risk assessment will support DHS's design and evaluation of alternative risk management strategies. The computational engine being developed by Battelle does not permit, let alone encourage, risk managers to explore "if resource allocation, then

[5] Attack trees and attack graphs are modeling techniques for understanding risk in complex situations. Both are graphical representations showing all ways to attack or damage a system. Decision trees are event trees with decisions represented as possible events. Attack-preference models examine decisions from the viewpoint of the attacker rather than the defender. See http://csdl2.computer.org/persagen/DLAbsToc.jsp?resourcePath=/dl/proceedings/&toc=comp/proceedings/itcc/2004/2108/01/2108toc.xml&DOI=10.1109/ITCC.2004.1286496. Accessed Nov. 1, 2006.

probable consequence" scenarios for evaluating alternative risk management strategies.[6] DHS needs to determine how strategies involving specific investments of resources in protection and countermeasures translate to changes in risk and impact terrorist plans and actions. Moreover, the model should have an interface and visualization component that makes its results and limitations easier to understand and be used by decision makers.

The committee encourages DHS to continue to build on, refine, and improve the probabilistic risk assessment foundation already laid down. The committee will continue to pursue these and additional topics in its review over the coming year.

[6] The DHS methodology, as reflected in software, actually does allow changes in assumptions; but this must be done through an analyst and would require a significant time delay and limit the range of alternatives that could be examined.

Methodological Improvements to the Department of Homeland Security's Biological Agent Risk Analysis

BACKGROUND

In recognition of potential bioterrorist threats, President George W. Bush issued Homeland Security Presidential Directive 10 (HSPD10), "Biodefense for the 21st Century,"[1] on April 28, 2004. The directive requires assessments of the biological weapons threat to the nation:

> Another critical element of our biodefense policy is the development of periodic assessments of the evolving biological weapons threat. First, the United States requires a continuous, formal process for conducting routine capabilities assessments to guide prioritization of our on-going investments in biodefense-related research, development, planning, and preparedness. These assessments will be tailored to meet the requirements in each of these areas. Second, the United States requires a periodic senior-level policy net assessment that evaluates progress in implementing this policy, identifies continuing gaps or vulnerabilities in our biodefense posture, and makes recommendations for re-balancing and refining investments among the pillars of our overall biodefense policy. The Department of Homeland Security, in coordination with other appropriate Federal departments and agencies, will be responsible for conducting these assessments.[2]

The first Department of Homeland Security bioterrorism risk assessment was completed on January 31, 2006, and the report documenting the analysis was published on October 1, 2006.[3] This assessment and report implemented the requirement of the National Strategy for Homeland Security,[4] issued in July 2002 by the Office of Homeland Security, and of HSPD10 for DHS to assess the biological weapons threat in coordination with other appropriate federal departments and agencies. At DHS's request, the National Research Council (NRC) established the Committee on Methodological Improvements to the Department of Homeland Security's Biological Agent Risk Analysis to provide a review, via two reports (interim and final), of the methodology used in DHS's report.

The committee's first meeting was held at the National Academies' Keck Center in Washington, D.C., on August 28-29, 2006. The appendix contains the agenda for that meeting. The committee heard and discussed presentations regarding risk analysis for biological pathogens by representatives of DHS, its National Biodefense Analysis and Countermeasures Center (NBACC), Battelle Memorial Institute, the White House Homeland Security Council, and the Homeland Security Center for Risk and Economic Analysis of Terrorism Events (CREATE). The recommendations and discussion below are based solely on those briefings; DHS's bioterrorism risk assessment was not made available to the committee in time for this interim report; however, the committee believes that these briefings included sufficient detail to adequately present the methodology used in the risk analysis.

NBACC has contracted with Battelle to produce a computational engine that assesses the "normalized risk" of 28 pathogens as that risk relates to death, morbidity, and direct economic costs.[5] In federal Fiscal Year 2007 (FY2007), DHS intends to improve and refine its probabilistic risk assessment (PRA). The committee has been asked to recommend possible directions for improvement, as well as to comment on the technical aspects of DHS's technique and the broader suitability of PRA. These

[1] Available at http://www.fas.org/irp/offdocs/nspd/hspd-10.html. Accessed Nov. 1, 2006.

[2] Available at http://www.fas.org/irp/offdocs/nspd/hspd-10.html. Accessed Nov. 1, 2006.

[3] *Bioterrorism Risk Assessment.* 2006. Biological Threat Characterization Center of the National Biodefense Analysis and Countermeasure Center. Washington, D.C.

[4] See www.dhs.gov/xlibrary/assets/nat_strategy_hls.pdf. Accessed Nov. 1, 2006.

[5] In general usage, the distinction between "direct" and "indirect" costs is not precise. "Direct" refers to costs such as those associated with closing a facility or controlling an epidemic. Other, or "indirect," costs are those that result from these actions, such as lost business associated with the closing of a facility or reduced productivity due to public health measures.

comments are intended to provide guidance to DHS for its work during FY2007. Specifically, the committee has been given the following charge for this interim report:

- Assess the adequacy of the DHS's current methodology as a foundation for the desired risk analysis capabilities;
- Identify any other risk analyses that rely on the major components of the existing methodology, probabilistic risk analysis and multi-attribute risk analysis, and which could guide DHS's future developments;
- Assess the feasibility of incorporating models of second-order economic effects into the methodology during FY07;
- Identify better methods, if any, for handling the high degrees of uncertainty associated with the risk analyses of biological agents;
- Recommend near-term improvements to enhance the transparency of the method and its usefulness to decision makers;
- Discuss how the methodology could be extended to risks associated with classes of agents, including enhanced or engineered agents that have yet to be developed; and
- Discuss the feasibility of extending the methodology to also serve as a framework for risk analysis of chemical or radioactive threats.

For this interim report, the committee was not able to address the last of these tasks—to examine risk analysis for chemical or radioactive threats—because the breadth of this task exceeds the information that could be provided during briefings to the committee in one meeting. That task, however, will be addressed in the committee's final report.

The committee's charge for its final report is as follows:

- Recommend how the methodology can incorporate changing probability distributions that reflect how various actors (e.g., terrorists, first responders, public health community) adjust their choices over time or in different contexts;
- Recommend further improvements to the consequence analysis component of the methodology, including its models of economic effects;
- Identify any emerging methods for handling large degrees of uncertainty (e.g., fuzzy logic, possibility analysis) that merit consideration for future incorporation;
- Recommend further improvements to the transparency and usability of the methodology;
- Discuss in more detail beyond the first report how the methodology could be extended to risks associated with classes of agents, including enhanced or engineered agents that have yet to be developed; and
- Discuss in more detail beyond the first report the feasibility of extending the methodology to also serve as a framework for risk analysis of chemical or radioactive threats.

This charge will require study of the issues addressed here in greater depth and with a view toward the longer term. The committee is confident, however, that the recommendations included in this interim report are appropriate and necessary in the near term. The committee's recommendations that follow address the general goal of improving methodology. Each recommendation relates to multiple elements of the charge, as noted in the accompanying text.

THE DHS BIOTERRORISM RISK ASSESSMENT

This interim report frequently refers to "risk" and activities surrounding its manipulation. For purposes of clarity, several definitions are given:

- *Risk*—the potential for realization of unwanted, adverse consequences to human life, health, property, or the environment, computed as the product of the probability of an event and the consequence of that event.
- *Risk analysis*—the overall process that involves risk assessment, risk perception, risk communication, and risk management. The hazards to be analyzed (e.g., physical, chemical, nuclear, radiological, and biological agents) may result from natural events (e.g., earthquakes and hurricanes), technological events (e.g., chemical accidents), and human activity (e.g., design and operation of engineered systems or attack by terrorists).
- *Risk assessment*—the scientific process of identifying hazards and quantifying their potential adverse consequences (magnitude, spatial scale, duration, and intensity) and associated probabilities including the uncertainties surrounding these estimates. Risk assessment may include a description of the cause-and-effect links among hazards and the nature of the interdependencies, vulnerabilities, and consequences.
- *Risk perception*—beliefs held by individuals or organizations about the risks of a hazard. Risk perception is concerned with psychological and emotional factors, which have been shown to have an enormous impact on behavior. Risk perception can be influenced by personal knowledge, experience, and beliefs; it can be affected by changing perceptions of the threat, the vulnerabilities, and/or the consequences; it may be influenced by information about hazards, risk assessments, risk policies, and risk management decisions.
- *Risk communication*—the process used by risk analysts, decision makers, policy makers, and intelligent adversaries to provide data, information, and knowledge to change the risk perceptions of individuals and organizations and enable them to assess the risk differently than they otherwise might. Risk communication needs must be considered when developing strategies for managing risk; thus any risk analysis methodology must take into account how affected individuals perceive and understand risk.
- *Risk management*—the process of constructing and evaluating strategies for reducing losses from future hazards and dealing with the recovery process should a disaster occur. Risk management strategies include a combination of options, such as providing information (i.e., risk communication), economic incentives (e.g., subsidies, fines), insurance, compensation, regulations, and standards. These strategies enable individuals and private-sector or public-sector organizations to transfer, mitigate, or accept their perceived risks. Risk management strategies can be evaluated by undertaking cost-benefit analyses to determine the trade-off between the reduction of risk and the costs of undertaking such measures. In evaluating a risk management strategy, one needs to be concerned with the way resources are allocated (i.e., efficiency considerations) as well as with the impact of these measures on different stakeholders (i.e., distribution or equity considerations).

The model used for the DHS bioterrorism risk assessment is a computer-based tool used for assessing the relative risk of terrorist use of each of 28 specific pathogens, identified in other sources. The methodology described below is an instance of probabilistic risk assessment, which is particularly well adapted for low-frequency, high-potential-consequence events for which there is no database sufficient to assess risk using statistical analysis of historical data.

The PRA used by DHS divides the spectrum of possible attacks into a discrete set of scenarios, or sequences of events, and for each scenario it provides an estimate of the scenario's probability of occurrence, consequences, and risk. Owing to the extremely large size of the sample space, Battelle sampled the events in the scenarios involving a particular pathogen, estimated the risk associated with that pathogen, and compared it with the risk of other pathogens in order to obtain risk relative to that of other pathogens.

Each scenario involves a chain of as many as 17 events, which can be partitioned into those characterizing the terrorist group's motivations and goals; those involving its methods and ability to acquire, produce, and transport the given bioagent; and those surrounding the attack and response to it. Each event is further given discrete characteristics. For instance, the event of target selection can be further decomposed into the selection of a large, open building; a small enclosure; a large, divided building; a large outdoor space; a water pathway; a food pathway; or a contact target such as a letter. The event tree[6] generated thus has millions of scenarios, or paths through the tree, for which the probabilities and consequences must be explicitly or implicitly calculated.

For each scenario, a range of consequences—measured in terms of illnesses, fatalities, and economic losses—must be computed, with a probability distribution over the range. The "consequence engine" used for these computations consists of a series of equations whose variables are derived from the properties of the pathogen, the details of the scenario, and the hypothesized U.S. response to the terrorist event. DHS is developing improved means to estimate the first- and second-order economic effects (as discussed later in this report). In addition, it is developing systems dynamics models of the ways in which the scenarios might unfold. The committee will review this systems dynamics approach in its final report.

Even from this brief description, it can be seen that the DHS model requires a large amount of information, much of which is uncertain. This information includes the known properties of the pathogens, estimates of the propensities of terrorists to take different actions, and estimates of the reactions of the affected population and of the timeliness and effectiveness of the government response. With the exception of known scientific information, the parameters are either estimated from historical experience or elicited from experts, often in the form of probability distributions.

RECOMMENDATIONS

For the most part, the analysis described in the previous section follows approaches considered technically sound and useful in other areas of risk analysis such as nuclear reactor safety and chemical safety. In validation of risk, PRA avoids many of the practical problems and difficulties that arise from other alternative methods such as fuzzy logic, the analytic hierarchy process, or worst-case analysis (Banks and Anderson, 2006; Laviolette et al., 1995).

Event-tree analysis, which is the basis of PRA, is a well-developed risk tool in nuclear reactor safety and many other, usually engineering, contexts (Lindley and Singpurwalla, 1986). The main concern of the committee is that the current PRA event-tree paradigm does not fully support any of the components of risk analysis. It does not include consideration of the actions of an intelligent and reactive adversary, which is required for a complete risk analysis. It makes no provision for risk perception. It does not allow the exploration by decision makers of "what-if" questions, which is needed for risk management.[7] DHS needs to provide analyses for a variety of purposes to a variety of customers, and all within the context of competing security demands in the short run, while taking into account the longer-run concerns that may change over time. Therefore, a necessary first step is to clarify the longer-term goals and objectives of bioterrorism risk analysis.

Recommendation 1: DHS should establish a clear statement of the long-term purposes of its bioterrorism risk analysis.

[6] An "event tree" is a visual representation of all events that can occur in a system. As the number of events increases, the picture fans out like the branches of a tree.

[7] The DHS methodology, as reflected in software, actually does allow changes in assumptions; but this must be done through an analyst and would require a significant time delay and limit the range of alternatives that could be examined.

In order to justify the current methodology as a foundation for future analyses, a clear statement of the long-term purposes of the bioterrorism risk analysis is needed to enunciate how it will support risk assessment, risk perception, and especially risk management decision making. Criteria and measures should be specified for measuring how well these purposes are achieved. Key issues to be addressed by such a statement should include the following: who the key stakeholders are; what their short- and long-term values, goals, and objectives are; how these values, goals, and objectives change over time; how the stakeholders perceive the risks; how they can communicate these risks more effectively; what they need from the risk assessment in order to make better (more effective, confident, rational, and defensible) resource-allocation decisions; and who should perform the analyses (contractors, government, both). Another important operational consideration is the determination of how DHS should incorporate new information in its analyses. The pace of change in biotechnology will require frequent and systematic updates of information used by the model. DHS issues “tailored assessments” to respond to unscheduled requirements, in addition to its biennial report, and it must be able to incorporate new intelligence information or technological change, for instance, in these analyses.

DHS’s purposes for its bioterrorism risk assessment must be supported by its customers, by the U.S. Congress, and by the scientific community, among others; thus, DHS should actively solicit the opinions of its stakeholders to ensure that communication on issues of risk analysis is two-way. To that end, the language and analyses used must be precise. The technical presentations given to the committee suggest that the model documentation does not always use standard and consistent terminology. For example, several speakers at the committee’s first meeting used the term “relative risk” to refer to what should be called “normalized risk,” and “likelihood” was sometimes used as a synonym for “probability.” The terms “risk,” “expected risk,” and “expected consequences” were often casually interchanged, and the computation of “normalized risk” was flawed.[8] The terms “illness” and “morbidity” should be clarified and defined more precisely (i.e., illness would need to be defined as either “infected” or “symptomatic”).

Other terms used in the presentations to the committee were not precisely defined, and functional notation was confusing. DHS should define and use a standard lexicon, clarify concepts, and align with contemporary literature in order to improve the transparency of its models and results. DHS’s operational definition of “risk” should be refined to include time explicitly—for example, by indicating how many events with various degrees of severity of adverse consequences can be expected over what time intervals if different risk management interventions are implemented. Attention also needs to be given to the uncertainty and ambiguity associated with these risks. Use of outside peer reviews may help in this regard. The issues raised here are not minor concerns; this lack of precision can lead to internal inconsistencies in the model and to communication problems at all levels.

DHS’s risk assessment currently encompasses what are mainly traditional bioagents. However, it seems logical that the DHS vision for risk analysis should be broad enough to include risks posed by other significant future biological threats. Traditional bioagents are “naturally occurring microorganisms or toxin products with the potential to be weaponized and disseminated to cause mass casualties.”.[9] Testing the methodology by using existing biological agent threat lists, as has been done to date, is a prudent and logical way to start, given the very large number of pathogens that could possibly be used as weapons. Existing threat lists (e.g., from the Centers for Disease Control and Prevention[10]) reflect

[8] After normalization (division by the average risk over all agents), information about the actual magnitude of the risk is lost, affecting risk assessment and making the analysis of most resource-allocation decisions difficult. Moreover, distributions of risk, as normalized in this way, cannot be created by simply normalizing the scale of the non-normalized risk.

[9] *Federal Register,* Vol. 71, No. 174, 2006, available at http:/www.hhs.gov/ophep/ophemc/bioshield/ PHEMCESStrategyFRNotice090806.pdf. Accessed Nov. 1, 2006.

[10] *Federal Register*, Vol. 71, No. 174, 2006, available at http://www.hhs.gov/ophep/ophemc/bioshield/ PHEMCEStrategyFRNotice090806.pdf. Accessed Nov. 1, 2006.

extensive experience and the judgment of the intelligence and scientific communities. However, many bioterrorism experts would agree that the "logic behind biowarfare programs of the past will not necessarily guide the life sciences as new technology rapidly emerges; biowarfare programs of the past predated current knowledge of molecular biology" (Relman, 2006, pp. 113-115). Therefore, future iterations of the methodology should also consider enhanced, emerging, and advanced agents in addition to traditional bioagents:

- *Enhanced agents* are those that are modified to circumvent current countermeasures—for example, microorganisms that are purposefully manipulated to be resistant to multiple antibiotics, thus complicating a public health response in the aftermath of an attack.
- *Emerging agents* are those that occur naturally but are newly recognized or anticipated to pose a public health threat—for example, a highly lethal and readily transmissible influenza strain that may cause a pandemic.
- *Advanced agents* are novel microorganisms that may be created by employing laboratory methods.

The results of such an extended risk assessment would be useful in determining the appropriate allocation of resources to develop flexible defenses—those that may be useful against a wide range of microorganisms that may share common processes in causing disease. Such an assessment would require information that is not currently available—estimates of likely developments in biotechnology that would enable new capabilities that could be used by terrorists. The committee believes that, for the near term, the elicitation of expert opinion, similar to what was undertaken in DHS's assessment of traditional bioagents, would be a useful starting point. This could be the first step in establishing the risk imposed by agents not yet in the environment and in broadening the analysis to include classes of agents rather than individual agents. The committee will examine this difficult problem in more depth in its final report.

Recommendation 2: DHS should improve its analysis of intelligent adversaries.

Event trees were not originally developed to model intelligent adversaries who adapt their attacks in response to (or in anticipation of) their opponents' defensive actions and/or in response to their own initial successes or failures in plan execution. Alternative risk analysis techniques, including attack-preference, decision-tree, attack-tree, or attack-graph models,[11] can complement or replace probability elicitation. There have been recent advances in dealing with interdependent and coordinated adversary actions, called interdependent security (Heal and Kunreuther, 2005), which may improve the fidelity of DHS models.

To use a PRA event-tree risk assessment in the analysis of intelligent adversaries, the tree must include all realistic threats that adversaries may pursue. The committee believes that the DHS PRA tree is reasonably complete, although DHS should examine this further in light of the expectation that adversaries will adapt to any defensive decisions made by the United States. A small number of well-chosen red teams (i.e., individuals including both technologists and those with experience in targeting and strategy, whose purpose is to simulate adversarial decision making) to provide input for "what-if" scenarios can help to confirm and expand the current state of understanding and model validation and can complement expert opinion.

[11] Attack trees and attack graphs are modeling techniques for understanding risk in complex situations. Both are graphical representations showing all ways to attack or damage a system. Decision trees are event trees with decisions represented as possible events. Attack-preference models examine decisions from the viewpoint of the attacker rather than the defender. See http://csdl2.computer.org/persagen/DLAbsToc.jsp?resourcePath=/dl/proceedings/&toc=comp/proceedings/itcc/2004/2108/01/2108toc.xml&DOI=10.1109/ITCC.2004.1286496. Accessed Nov. 1, 2006.

The probabilities in the event tree must be of sufficient quality to produce trustworthy results. Most of the event probabilities have been generated using expert opinion. DHS is keenly aware that this approach may be unreliable, and the committee is pleased that DHS intends to use CREATE's expertise to improve elicitation of the views of subject-matter experts. But the reliability of these probability assessments will always be problematic, requiring careful attention to the elicitation methods as well as needing well-designed sensitivity analyses (Kahneman and Tversky, 2000; Meyer and Booker, 2001). Moreover, strictly probabilistic analysis should also be supplemented with other methods, such as attack-preference models and attack-tree models, in order to ascertain any severe contradictions in the resulting risk management (or mitigation) recommendations.

The Mission Oriented Risk and Design Analysis (MORDA) model, used in several Department of Defense risk assessment studies, is an example of the use of subject-matter expert teams from various disciplines to collect data and incorporate expert knowledge about adversaries. The MORDA model uses this collected information in adversary models and attack-tree models (Buckshaw et al., 2005).

In order to better understand the sources of uncertainty and to plan for their reduction, any analysis resulting from the PRA model should include a data-quality matrix with a qualitative assessment of the sources and quality of the data and perhaps quantitative indications of the confidence and precision associated with current estimates (e.g., plausible range of values for model inputs) for the 28 bioagents and the 17 steps in the event tree developed by Battelle.

The committee believes that static probabilities, as they are currently used by DHS, are insufficient to model the behavior of intelligent adversaries. Static probabilities may be appropriate when dealing with nuclear reactors, but not for an intelligent adversary who adapts an attack on the basis of the actions of the defenders and on information that it acquires as planning and execution progress. Although classical game theory is a formal way to handle such situations, there is now a growing literature that may be more relevant for dealing with the adversarial nature of the bioterrorism problem (Bier et al., 2005; Enders and Sandler, 2006; Heal and Kunreuther, 2005). Studies have been conducted by the Navy Postgraduate School in which the defender computed a strategy that would minimize the maximum damage that could be caused by an attacker (terrorist) who was aware of that strategy. These "attacker-defender" studies, which have been undertaken in various contexts to determine how best to protect U.S. infrastructure, might serve to complement the static probability analyses currently used by DHS (Brown et al., in press).

Any analysis of adversarial actions, as well as of mitigation strategies and responses, will require accurate estimates of the real damages that the United States would experience. Currently, the PRA computes measures of mortality, morbidity, and direct economic costs. But indirect economic costs (e.g., of business interruption) must also be included to avoid underestimating true financial consequences. If these indirect costs are large, it may be necessary to evaluate their impact, taking into account risk aversion and/or loss aversion.[12]

Evaluation of these costs will require that DHS more carefully consider its consequence measures and modeling, which should be augmented to include indirect economic effects. DHS is planning to use input-output models and CREATE-developed general equilibrium models to improve its estimates of the direct economic consequences of terrorist events in its FY08 risk assessment. Both of these techniques can be used to estimate the indirect costs. The committee agrees that their use is appropriate for the next stage of model development.

DHS is planning, however, to pursue consequence modeling that is of higher fidelity and resolution than that of the modeling being used now. Such a path is not clearly justified by either data availability or currently articulated decision needs. More fine-grained and detailed consequence models of targets should only be pursued if such granularity directly supports improved risk management decision making.

[12] Risk aversion is the reluctance of a person to accept a bargain with an uncertain payoff rather than another bargain with a more certain, but possibly lower, expected payoff. Loss aversion refers to the tendency for people to strongly prefer avoiding losses to acquiring gains.

The committee is concerned about the use of too fine a granularity in the simulation. It could result in false precision that might be mistaken for accuracy in a model that is, by necessity, not particularly well validated, affecting both risk assessment and risk management. In addition, too fine a granularity decreases the transparency of the model. The committee is concerned that merely increasing the number of parameters that need to be elicited may not increase the real or useful precision of the model.

Individuals' perceptions of risks can have a major influence on indirect economic consequences, resulting in a need to develop strategies to manage risk perception and to deal with these perceptions. DHS should consider decision-analytic methods for dealing with issues such as attitudes toward probabilities and consequences (the components of risk), the role of affect and emotion, biases in judgment, and the types of rules used by individuals and groups in choosing between alternatives.

Recommendation 3: DHS should increase its risk analysis methodology's emphasis on risk management.

Risk managers should be able to explore the impact of different investment strategies on the effects they might have on the attacker. Typical trade-offs facing U.S. risk managers might involve allocating resources among human intelligence versus vaccine development or deployment of biohazard sensors. A given resource allocation may drive a corresponding set of decisions by potential terrorists, which in turn changes risks. The current DHS event-tree PRA is not adequate for such risk management purposes. This is so because the event-tree PRA cannot determine which portfolio of investments is most effective and how potential attackers are likely to respond, although it does provide value in giving a coarse look at relative risks. This inadequacy highlights the importance of improving the current risk analysis with red teaming, attack-preference models, attack-tree models, and perhaps, game-theoretic analyses or alternatives. All of these techniques will serve to mitigate the high degree of uncertainty associated with the risk analysis of biological agents.

It is unclear to the committee how the current PRA approach supports DHS's design and evaluation of alternative risk management strategies. The computational engine does not permit, let alone encourage, risk managers to explore scenarios of "if resource allocation, then probable consequence." DHS needs to determine how alternative risk management strategies, involving specific resource investments in attack prevention, consequence mitigation, or other forms of protection, translate to changes in the overall level of risk. An interface and visualization component is needed to display results and limitations of this very complex model and to improve transparency.

In evaluating alternative risk management strategies, DHS should take into account all significant benefits that result from any strategy, beyond just those benefits that directly impact the risks of bioterrorism attacks. For instance, investment in intelligence might include all homeland security risks, and the risk management trade-offs should be considered in that larger context. This last conclusion has ramifications for all of DHS's risk analysis and directly addresses the committee's final charge. It will be more fully explored in this study's final report.

DHS should develop a targeted research program to develop risk analysis methods that take into account the decision maker's risk perception and risk management strategies. Such a program would include the following, for example: consideration of how constraints on resources available to the decision maker might affect terrorist decisions, and an understanding of how attackers who encounter failures or setbacks in executing an initial plan will respond—including the realistic possibility that they will implement contingency plans or adaptively replan to achieve goals that still appear feasible and worthwhile.[13] Methods for modeling multiple coordinated attacks by teams of adversaries should also be considered.[14] These changes should all be incorporated into the next generation of DHS's bioterrorism risk assessment and management technologies. The committee believes that these extensions can be achieved by expanding the models rather than by increasing the fidelity of existing models.

[13] See http://handle.dtic.mil/100.2/ADA009141. Accessed Nov. 1, 2006.

[14] See http://www.rms.com/Publications?QuanTerRisk4Portfolios_Woo_Aon.pdf. Accessed Nov. 1, 2006.

SUMMARY

As previously noted, each of the committee's recommendations relates to multiple elements of its charge. Here, responses to each element of the charge, in order, are summarized.

- DHS's current methodology is adequate but incomplete. A statement of purpose is needed, as well as methods to handle intelligent adversaries. Red teaming, attack-preference models, attack-tree models, and game-theoretic analyses should all be examined for the purpose of supplementing the existing methodology.
- The analyses cited, by Buckshaw et al. (2005) and by Brown et al. (in press), are examples of other types of risk analysis that would be appropriate for DHS's future development.
- DHS's current plans for the incorporation of second-order indirect economic effects into its methodology are appropriate, as long as the model's level of granularity is carefully considered.
- High degrees of uncertainty can be addressed by the incorporation of red teaming, attack-preference models, attack-tree models, and game-theoretic analyses. The incorporation of data-quality matrices in DHS's analyses will lead to a better understanding of the sources of uncertainty.
- In order to improve transparency, DHS should define and use a standard lexicon, clarify concepts, and align with the contemporary literature.
- In order to extend the methodology to risks associated with classes of agents, careful elicitation of expert opinion is the best starting point. This issue will be further examined in the committee's final report.
- No examination was made in this interim report of the feasibility of extending the methodology to serve as a framework for risk analysis of chemical or radioactive threats.

REFERENCES

Banks, D., and S. Anderson. 2006. "Combining Game Theory and Risk Analysis in Counterterrorism: A Smallpox Example." Pp. 9-12 in A. Wilson, G. Wilson, and D. Olwell, eds., *Statistical Methods in Counterterrorism.* New York: Springer.

Bier, Vicki, Santiago Oliveros, and Larry Samuelson. 2005. "Choosing What to Protect: Strategic Defense Allocation Against an Unknown Attacker." University of Wisconsin Working Paper.

Brown, G., W. Matthew Carlyle, Javier Salmeron, and Kevin Wood. In press. "Defending Critical Infrastructure." *Interfaces*.

Buckshaw, Donald L., Gregory S. Parnell, Willard L. Unkenhotz, Donald L. Parks, James M. Wallner, and O. Sami Saydjari. 2005. "Mission Oriented Risk and Design Analysis of Critical Information Systems." *Military Operations Research* 10(2): 19-38.

Enders, Walter, and Todd Sandler. 2006. *The Political Economy of Terrorism.* Cambridge: Cambridge University Press.

Heal, Geoffrey, and Howard Kunreuther. 2005. "You Only Die Once: Interdependent Security in an Uncertain World." Pp. 35-36 in H.W. Richardson, P. Gordon, and J.E. Moore II, eds., *The Economic Impacts of Terrorist Attacks*. Cheltenham, U.K.: Edward Elgar.

Kahneman, Daniel, and Amos Tversky. 2000. *Choices, Values and Frames.* New York: Cambridge University Press.

Laviolette, Michael, John W. Seamon, Jr., J. Douglas Barrett, and William H. Woodall. 1995. “A Probabilistic and Statistical View of Fuzzy Methods.” *Technometrics* 37: 249-261.

Lindley, Dennis V., and Nozer D. Singpurwalla. 1986. “Reliability and Fault Tree Analysis Using Expert Opinions.” *Journal of the American Statistical Association* 81: 87-90.

Meyer, M.A., and J.M. Booker. 2001. *Eliciting and Analyzing Expert Judgment: A Practical Guide*. ASA-SIAM Series on Statistics and Applied Probability, Vol. 7. Philadelphia, Pa.: Society for Industrial and Applied Mathematics.

Relman, D.A. 2006. “Bioterrorism—Preparing to Fight the Next War.” *New England Journal of Medicine* 354: 113-115.

Appendix

AGENDA FOR COMMITTEE MEETING, AUGUST 28-29, 2006

KECK CENTER OF THE NATIONAL ACADEMIES

**500 Fifth Street, N.W.
Washington, DC 20001**

Monday, August 28, 2006

Closed Session (committee members and NRC staff only)

8:00 a.m.

Data-Gathering Session Open to the Public

9:45 a.m.	Introductory Remarks	Department of Homeland Security Science and Technology Leadership
10:00 a.m.	Biology Presentation (background for non-biologists)	Prof. Luciana Borio, University of Pittsburgh, Center for Biosecurity
10:45 a.m.	Break	
11:00 a.m.	DHS and National Biodefense Analysis and Countermeasures Center (NBACC) Background and Risk Assessment Requirements	Dr. Steven Bennett, DHS/NBACC Dr. Bernard Courtney, DHS/NBACC
11:30 a.m.	DHS 2006 Bioterrorism Risk Assessment Methodology	Dr. Richard Denning, Battelle Memorial Institute
1:00 p.m.	Lunch	
1:45 p.m.	Past Experiences and Implications for Bioterrorism	Prof. Detlof von Winterfeldt, Director, Center for Risk and Economic Analysis of Terrorism Events (CREATE), University of Southern California
2:15 p.m.	Assessing the Economic Impacts of Terrorism—Capturing Behavioral Linkages and Resilience	Prof. Adam Rose, Pennsylvania State University and CREATE
2:45 p.m.	Break	

Data-Gathering Session Open to the Public: Scenario Analysis and Consequence Modeling

3:00 p.m	Branch Probabilities and Uncertainty Management	Mr. Rob Carnell, Battelle
	Atmospheric (Outdoor) Dispersion Modeling	Ms. Mary Shell, Battelle
	Indoor Aerosol Dispersion Modeling	Dr. Brian Hawkins, Battelle
	Medical Mitigation and Epidemiological Modeling	Ms. Traci Hale and Dr. Nancy McMillan, Battelle
	Food and Water Contamination Modeling	Mr. Jon David Sears, Battelle
	Risk Calculation Engine	Mr. Rob Carnell, Battelle
5:30 p.m.	Reception	

Tuesday, August 29, 2006

Data-Gathering Session Open to the Public

9:30 a.m.	Updates and Planned Changes for the 2008 Bioterrorism Risk Assessment	DHS/NBACC, Battelle Staff
10:45 a.m	Break	

Closed Session (committee members and NRC staff only)

4:00 p.m. Adjourn