Biosecurity and Bioterrorism: Biodefense Strategy, Practice, and Science
Volume 6, Number 4, 2008 © Mary Ann Liebert, Inc.
DOI: 10.1089/bsp.2008.0930

COMMENTARY

SCIENTISTS URGE DHS TO IMPROVE BIOTERRORISM RISK ASSESSMENT

Gregory S. Parnell, Luciana L. Borio, Gerald G. Brown, David Banks, and Alyson G. Wilson

In 2006, the Department of Homeland Security (DHS) completed its first Bioterrorism Risk Assessment (BTRA), intended to be the foundation for DHS's subsequent biennial risk assessments mandated by Homeland Security Presidential Directive 10 (HSPD-10). At the request of DHS, the National Research Council established the Committee on Methodological Improvements to the Department of Homeland Security's Biological Agent Risk Analysis to provide an independent, scientific peer review of the BTRA. The Committee found a number of shortcomings in the BTRA, including a failure to consider terrorists as intelligent adversaries in their models, unnecessary complexity in threat and consequence modeling and simulations, and a lack of focus on risk management. The Committee unanimously concluded that an improved BTRA is needed to provide a more credible foundation for risk-informed decision making.

"The threat posed by biological agents employed in a terrorist attack on the United States is arguably the most important homeland security challenge of our era. Whether natural pathogens are cultured or new variants are bioengineered, the consequence of a terrorist-induced pandemic could be millions of casualties—far more than we would expect from nuclear terrorism, chemical attacks, or conventional attacks on the infrastructure of the United States such as the attacks of September 11, 2001. Even if there were fewer casualties, additional second-order consequences (including psychological, social, and economic effects) would dramatically compound the effects. Bioengineering is no longer the exclusive purview of state sponsors of terrorism; this technology is now available to small terrorist groups and even to deranged individuals."

—Department of Homeland Security's Biological Threat Risk Assessment:
A Call for Change, National Research Council, 2008

DHS'S FIRST BIOLOGICAL THREAT RISK ASSESSMENT

Risk assessment (the quantification of risk) is the foundational element of risk analysis, which also includes risk communication (the provision of information about risks) and risk management (strategies for reducing future losses).[1-3] Quantifying risk is the prerequisite for effective risk communication to policymakers and stakeholders, and for supporting critical risk management decisions by all lev-

Gregory S. Parnell, PhD, is Professor of Systems Engineering, Department of Systems Engineering, United States Military Academy, West Point, New York. Luciana L. Borio, MD, is Senior Associate, Center for Biosecurity of the University of Pittsburgh Medical Center, Baltimore, Maryland. Gerald G. Brown, PhD, is Distinguished Professor, Operations Research Department, Naval Postgraduate School, Monterey, California. David Banks, PhD, is Professor of the Practice of Statistics, Department of Statistics and Decision Science, Duke University, Durham, North Carolina. Alyson G. Wilson, PhD, is Associate Professor, Department of Statistics, Iowa State University, Ames, Iowa.

Report Documentation Page

Form Approved
OMB No. 0704-0188

Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
2008		**00-00-2008 to 00-00-2008**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Scientists Urge DHS to Improve Bioterrorism Risk Assessment	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Naval Postgraduate School,Operations Research Department ,Monterey,CA,93943**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**Same as Report (SAR)**	**4**	

els of government and the private sector. Because it is not possible to fully protect every target and community against every potential threat, we need to identify the greatest risks and take the most efficient steps to reduce them.

Homeland Security Presidential Directive 10 (HSPD-10): Biodefense for the 21st Century,[4] issued in April 2004, states that "[b]iological weapons in the possession of hostile states or terrorists pose unique and grave threats to the safety and security of the United States and our allies" and charges the Department of Homeland Security (DHS) with issuing biennial assessments of biological threats, to "guide prioritization of our on-going investments in biodefense-related research, development, planning, and preparedness."[4] The subsequent Homeland Security Presidential Directive 18 (HSPD-18): Medical Countermeasures against Weapons of Mass Destruction[5] calls for an integrated risk assessment of all chemical, biological, radiological, and nuclear (CBRN) threats.

In 2006, DHS completed its first risk assessment and published *Bioterrorism Risk Assessment* (BTRA).[6] The work was contracted to Battelle Memorial Institute in Columbus, Ohio. The BTRA report resulted from a complex federation of integrated computer-based models to estimate the risks associated with the intentional terrorist release of each of 27 natural pathogens[7] and one engineered agent (multidrug resistant *Bacillus anthracis*). The BTRA ranks each pathogen according to its level of risk, based on subjective event probabilities and their consequences. The subjective event probabilities were elicited from dozens of biological weapons experts. Event consequences were estimated from a number of different models and simulations. For example, to estimate the spread and health effects of infectious diseases, "susceptible, exposed, infected, and removed" (SEIR) mathematical models for the relevant diseases were employed (see Bailey[8] for a comprehensive treatment).

DHS promotes the BTRA of 2006 as an "end-to-end risk assessment of the bioterrorism threat," ranking various agents by their level of risk, to "assist and guide biodefense strategic planning."[6] The intent of BTRA is that it could be used to identify vulnerabilities to particular agents or scenarios, or to prioritize federal investment in particular countermeasures. Moreover, the BTRA methodology is intended to be the foundation for future biennial risk assessments by DHS and perhaps to be applied to other areas such as chemical or nuclear terrorism, fulfilling DHS's obligations to HSPD-10 and HSPD-18.

NRC Committee Finds Serious Limitations with DHS's BTRA

At the request of DHS, the National Research Council established the Committee on Methodological Improvements to the Department of Homeland Security's Biological Agent Risk Analysis to provide an independent, scientific peer review of the BTRA. The Committee reviewed all of the details in the BTRA of 2006, interviewed its leaders and its implementers, held discussions with other experts who had not themselves participated in the BTRA, and received briefings from DHS on planned improvements to the subsequent BTRA of 2008. In accord with HSPD-10, the Committee reviewed not only the mathematical foundation of the BTRA, but also its potential utility to policymakers.

The NRC Committee's review was limited to the initial BTRA of 2006 because the Committee's deliberations ended before the BTRA of 2008 report was released. Although the updated BTRA of 2008 included a number of additions and refinements to the BTRA of 2006, none of the changes would alter the Committee's assessment of the BTRA methodology or render the Committee's findings irrelevant.

The Committee identified a number of fundamental problems with the BTRA, ranging from the use of unnecessarily complicated probability models, to simplistic assumptions regarding the manner in which terrorist behavior should be modeled.[9] The Committee also unanimously judged the BTRA unsuitable for risk management. In their final report, the Committee made detailed recommendations as to ways DHS could remediate the BTRA's many shortcomings.

DHS Failed to Adequately Model the Behavior of Terrorists as Intelligent Adversaries

Fortunately, bioterrorism attacks have been so infrequent that we have limited data on which to draw. However, as 9/11 demonstrated, terrorists will certainly design their attacks to exploit our vulnerabilities and attempt to achieve consequences that will meet their objectives. Therefore, homeland security risk analysts must consider the potential decisions of terrorists as if they were intelligent adversaries.

However, the BTRA does not consider the range of possible attack strategies that an intelligent adversary might pursue. Instead, the BTRA uses an event tree, representing many hypothetical sequences of events, from the terrorist decision to initiate an attack to the consequences of the attack. It represents terrorist decisions by means of probabilities assessed by experts as they would assess the probability of a natural hazard (eg, an earthquake) or an engineered system failure (eg, a nuclear reactor). For example, in the BTRA experts assign subjective probabilities for terrorists selecting a target, selecting a pathogen, acquiring the pathogen, etc. Each of these events is associated with a very small probability. To assess the expected consequences of each scenario, the assigned small probability of each event must

be multiplied for every event in the scenario. This yields a small number, minimizing the true consequences of each threat.

An analogy to the events of 9/11 might be useful here. If the BTRA were to be used to characterize the threat of 9/11, experts would have assigned probabilities for Al-Qaeda to choose the World Trade Center towers as the target and planes as the weapon. These small probabilities, when multiplied by the number of deaths caused by such an attack, would have resulted in a very small number, and the risk of such attack would have been deemed insignificant. However, terrorists, our intelligent adversaries, did not assign probabilities to each of their choices. Terrorists are goal-oriented, resourceful adversaries, who will, given the constraints they perceive, select the best agent and target to achieve their objectives.

The Complexity of the DHS Consequence Models Is Not Supported by Existing Knowledge

The Committee closely examined the assumptions and the mathematical details of the BTRA and found weaknesses in model conception and unnecessary complexity throughout, along with errors in enough of the underlying mathematics and statistics that the Committee was compelled to express significant concern.

Examples of unnecessary complexity include the large number of events in each tree and the overly elaborate algorithm with which outcome probabilities are calculated. Additionally, the SEIR models used to analyze the health consequences of various attack scenarios require input parameter values for which empirical data do not exist. Because the granularity of detail in the SEIR models cannot be supported by existing clinical and epidemiologic data for any pathogen on the BTRA list—not even *B. anthracis*—many broad assumptions are required. This results in an illusion regarding the precision of the results when there is none.

BTRA Does Not Focus on Risk Management

Risk assessment requires an estimate of the threat (based on the intentions and capabilities of adversaries) and the expected magnitude of consequences (eg, deaths, illnesses, and economic losses) given our vulnerabilities. Alone, complex biennial risk assessments, such as the BTRA, have no direct impact on risk reduction. In addition, the risk has to be communicated to the stakeholders and policymakers. In the end, only effective risk management strategies can reduce risk.

However, the current versions of the BTRA present significant barriers to stakeholders who should be using the BTRA for risk management. The tool's construction and assumptions are not transparent, the interface is not user-friendly, and the tool does not easily allow modeling of alternative scenarios and evaluation of various risk management strategies. Given the large number of homeland security stakeholders who influence the vulnerabilities and, as a result, the consequences of a biological attack, it is critically important that DHS revise its tool so that these stakeholders can assess the potential effects of their risk management strategies.

The Call for Change

The threat of bioterrorism is significant; various pathogens could cause unprecedented harm to the health and prosperity of Americans, and the technical barriers to launching effective biological attacks are not insuperable, even for small groups or individuals. Thus, the objectives of the BTRA are essential and laudable. But given the defects in the BTRA's underlying model and user interface, the Committee concluded that the current incarnation of the BTRA is inadequate, does not satisfy the intent of HSPD-10, and should not be used as the foundation for future biennial risk assessments or expanded to an integrated risk assessment of CBRN threats. The Committee unanimously believes that an improved BTRA is needed to provide a credible foundation for risk-informed decision making.

What DHS Should Do

A flawed probabilistic risk assessment tool is inadequate to communicate risk and to support risk management decisions. The risk of a bioterrorism attack requires the best efforts of our homeland security community. The authors believe that DHS should take 3 *near-term actions* to make the necessary changes to BTRA:

1. **Form an *independent* senior technical review panel to advise the DHS risk analysis team leaders.** The DHS risk assessment is a critical challenge that requires expertise in many technical disciplines (including risk analysis, biology, epidemiology, statistics, operations research, social science, and economics) to develop credible and responsive risk assessment models. The senior review panel should guide the risk analysis team in the implementation of the required changes described in the NRC report and review the BTRA output. Further, this review panel should communicate to government leaders and stakeholders DHS's progress in revising the BTRA.
2. **Obtain robust stakeholder input and feedback.** DHS must meaningfully engage with stakeholders and incor-

porate their feedback into the BTRA. Many in government and public and private organizations need to participate in the bioterrorism risk assessment to understand their vulnerabilities, the potential consequences of attack, and the effectiveness of mitigation strategies. The results of the assessments should directly inform their risk management decisions.

3. **Develop and incorporate risk analysis techniques that model terrorists as intelligent adversaries.** The NRC report proposed 3 possible techniques to assess the impact of an intelligent adversary. What these techniques share is that instead of requiring the analyst to input probabilities of what the terrorist is likely to do, they instead output the terrorist actions that will best achieve the terrorists' objectives. The 3 techniques include: (1) a "bioterrorism decision model" to model terrorist actions and U.S. strategic actions as decisions, and agent acquisition, employment, vulnerabilities, consequences, and mitigation events as uncertain events using available off-the-shelf software (eg, see Decision Analysis Software Survey, http://Lionhrtpub.com/orms/surveys/das/das.html); (2) a tri-level decision support model to allocate defensive investments (visible to the attacker) that represent an attacker's reasonable response to observing these preparations, and reactions to any attack with the resources made available by the defensive investments; and (3) a game-theoretic model of the adversaries that randomizes expected consequences to capture the variability of outcomes. These are not mere theoretical suggestions, but rather substantive tools and methods drawn from extensive research and experience in the military and in the private sector that can significantly improve the credibility and usefulness of the BTRA. We recommend that these 3 techniques (or others that achieve the same objectives) be developed and evaluated as soon as possible. Insights from multiple credible models may be the best way to ensure that homeland security decision makers have the best available data for informed decision making.

In their report to the National Research Council, the Committee has made further detailed and technical recommendations that would improve the BTRA.[9] The Committee hopes DHS will now complete the steps necessary to produce a robust and reliable risk assessment to meet this urgent need.

Disclaimer and Acknowledgments

The views expressed in this article are those of the authors and do not reflect the official policy or position of the United States Army, the United States Navy, the Department of Defense, Los Alamos National Laboratory, the National Research Council, or the Department of Homeland Security.

The authors, all members of the NRC Committee, acknowledge the contributions of our other colleagues on the NRC Committee and the NRC staff, especially Neal Glassman and Scott Weidman. We also gratefully acknowledge the suggestions of 3 reviewers. However, unless specifically stated as the recommendation of the Committee, the views presented in the article are those of the authors.

References

1. National Research Council, Committee on the Institutional Means for Assessment of Risks to Public Health. *Risk Assessment in the Federal Government: Managing the Process.* Washington, DC: National Academies Press; 1983.
2. Stern PC, Fineberg HV, eds.; Committee on Risk Characterization, National Research Council. *Understanding Risk: Informing Decisions in a Democratic Society.* Washington, DC: National Academies Press; 1996.
3. Byrd DM, Cothern R. *Introduction to Risk Analysis: A Systematic Approach to Science-Based Decision Making.* Lanham, MD: Government Institutes; 2000:329-355.
4. The White House. Homeland Security Presidential Directive 10 [HSPD-10]: Biodefense for the 21st Century. 2004. www.fas.org/irp/offdocs/nspd/hspd-10.html. Accessed January 16, 2008.
5. The White House. Homeland Security Presidential Directive 18 [HSPD-18]: Medical Countermeasures Against Weapons of Mass Destruction. 2007. www.fas.org/irp/offdocs/nspd/hspd-18.html. Accessed January 16, 2008.
6. U.S. Department of Homeland Security. 2006. *Bioterrorism Risk Assessment.* Fort Detrick, MD: Biological Threat Characterization Center of the National Biodefense Analysis and Countermeasures Center (U); 2006. Document originally classified SECRET, but portions declassified for NRC publication.
7. Rotz LD, Khan AS, Lillibridge SR, Ostroff SM, Hughes JM. Public health assessment of potential biological terrorism agents. *Emerg Infect Dis* 2002;8(2):225-230.
8. Bailey NTJ. *The Mathematical Theory of Infectious Diseases and Its Applications.* London: Griffin; 1975.
9. National Research Council, Committee on Methodological Improvements to the Department of Homeland Security's Biological Agent Risk Analysis. *Department of Homeland Security Bioterrorism Risk Assessment: A Call for Change.* Washington, DC: National Academies Press; 2008. http://www.nap.edu/catalog.php?record_id=12206.

Address correspondence to:
Gregory S. Parnell, PhD
Professor of Systems Engineering
Department of Systems Engineering
United States Military Academy
West Point, NY 10996

E-mail: gregory.parnell@usma.edu