Biowar and Bioterrorism Risk Assessment

Philip V. Fellman
Sawyer Business School,
shirogitsune99@yahoo.com

Gregory S. Parnell
Innovative Decisions
gparnell@innovativedecisions.com

Kathleen M. Carley
Carnegie Mellon University
kathleen.carley@cs.cmu.edu

In this paper we follow our earlier work on the mathematical and computational modeling of biological warfare and its potential extensions to nuclear terrorism. In particular we review Dr. Parnell's earlier critique of the proper and improper use of probabilities, scenarios and the emergent properties of terrorism undertaken in conjunction with the National Academy of Sciences, the National Academy of Engineers and the National Institute of Health. As indicated in the earlier report published by the National Academies Press (http://books.nap.edu/openbook.php?record_id=12206&page=3) we extend the argument that: "The DHS (2006) report and DHS presentations of its content use inconsistent, imprecise technical language and do not define many key terms." In addition we propose an improved model of biological warfare developed by Dr. Carley and provide additional analysis of terrorism with respect to weapons of mass destruction.

1 Introduction

Assessing the risk of terrorism, and terrorist threats is a difficult and complex undertaking. As we have argued elsewhere (Fellman, 2011), official government estimates produced by national boards have a tendency to use probabilistic language in a rather loose fashion, placing excessive emphasis on often ill-defined or incomplete analytical models. In this paper, we review some of the methodological difficulties highlighted by the National Research Council Report "Department of Homeland Security Bioterrorism Risk Assessment: A Call for Change" which analyzed the approach of the Department of Homeland Security's 2006 Bioterrorism Threat Risk Assessment program.[1]

Following this review, we explore two alternative approaches for more carefully and usefully modeling bioterrorism threats, Intelligent Adversary Risk Analysis, as developed by Parnell, Smith and Moxley (2009), and Merrick and Parnell (2011) as well as the Biowar model developed by Carley (2011).

1.1 The Committee's Overview – Fundamental Flaws in the Methodology of BTRA 2006

The section below has been excerpted directly from the NRC report in order to share the committee's overview of the bioterrorism threat risk assessment process. The report was undertaken through a contract between the Department of Homeland Security and the National Research Council. The NRC was commissioned to carry out a study to recommend improvements to the methodology used for DHS' first (2006) Bioterrorism Risk Assessment.

> The Committee on Methodological Improvements to the Department of Homeland Security's Biological Agent Risk Analysis was established by the National Research Council and convened in August 2006 to review the Department of Homeland Security's (DHS's) Biological Threat Risk Assessment (BTRA) of

[1] In 2004, the President issued a homeland security directive that, along with the National Strategy for Homeland Security published in 2002, mandated assessments of the biological weapons threat to the nation and assigned responsibility for those assessments to the Department of Homeland Security (DHS). The first such assessment—the Biological Threat Risk Assessment (BTRA) of 2006—is a computer-based tool to assess the risk associated with the release of each of 28 biological threat agents. To assist in its preparation of this version of BTRA as well as the 2008 version, DHS asked the NRC to carry out a study of the methodology used by the agency to prepare BTRA of 2006. This NRC report presents an introduction to the challenge; an analysis of the critical contribution of risk analysis to risk management; a description of the method used to produce the BTRA of 2006, which is the foundation for later assessments; a discussion of risk assessment for unknown and engineered bio-threats; and ways to improve bioterrorism consequence assessment and the BTRA methodology. (from "Department of Homeland Security Bioterrorism Risk Assessment: A Call for Change, Committee on Methodological Improvements to the Department of Homeland Security's Biological Agent Risk Analysis, National Research Council, ISBN: 0-309-12029-2, 92008) http://www.nap.edu/catalog/12206.html

> 2006. The BTRA is a computer-based tool that has been applied by DHS to assess the risk associated with the intentional release of each of 28 biological threat agents categorized by the Centers for Disease Control and Prevention. The committee has identified a number of fundamental concerns with the BTRA of 2006, ranging from mathematical and statistical mistakes that have corrupted results, to unnecessarily complicated probability models and models with fidelity far exceeding existing data, to more basic questions about how terrorist behavior should be modeled. All of these issues are covered in the body of this report. Rather than merely criticizing what was done in the BTRA of 2006, the committee sought outside experts and collected a number of proposed alternatives that it believes would improve DHS's ability to assess potential terrorist behavior as a key element of risk-informed decision making, and it explains these alternatives in the specific context of the BTRA and the bioterrorism threat.

In at least one sense, the models which we present in sections three and four of this paper represent a practical continuation of the NRC critique of DHS' BTRA 2006. While DHS has already produced subsequent estimates in 2008 and a BAA calling for proposals in 2009, there has been a remarkably conservative adherence to the original methodology in the BTRA 2006 despite the criticisms and concerns voiced by the national academies and the NRC report.

1.2 The Intent of BTRA 2006

The model used by DHS for BTRA 2006 was a computer-based tool designed to assess the relative likelihood and consequences of terrorists' employing each of the 28 specific pathogens identified by CDC as possible terrorist threats. This methodology relied upon largely static probabilities and treated the probabilistic occurrence of an attack as being essentially similar to modeling the risk of an uncertain hazard rather than modeling the behavior of an intelligent adversary. A constructive methodology for intelligent adversary modeling is presented in section three of this paper, where we discuss the Parnell, Smith and Moxley model.

Additional description of the intent of BTRA 2006 is provided by the executive summary of the NRC report:

> DHS intended that the BTRA of 2006 be an "end-to-end risk assessment of the bioterrorism threat" with potential catastrophic consequences to human health and the national economy and that it "assist and guide biodefense strategic planning" (DHS, 2006, Ch. 1, p. 1) in response to the HSPD-10 directive to "conduct biennial assessments of biological threats." Guided by DHS's customers for information from the assessment, the BTRA of 2006 was designed to produce assessments in the form of risk-prioritized groups of biological threat agents. These prioritized lists could then be used

> to identify gaps or vulnerabilities in the U.S. biodefense posture and make recommendations for rebalancing and refining investments in the overall U.S. biodefense policy. DHS has assembled a confederation of researchers and subject-matter experts and is collaborating with national laboratories that can contribute to expanding the knowledge base of bioterrorism.

While BTRA 2006 was designed as a comprehensive treatment of bioterrorism, in practice it fell far short of the mark. Following the basic critique summarized above, the NRC report actually recommended that BTRA 2006 not be used as the methodology for dealing with bioterrorism (p. 2):

> The committee met on August 28-29, 2006, with representatives of DHS in response to a DHS request for guidance on its near-term BTRA development efforts. In November 2006, in response to that request and based on the information it had received at the 2-day meeting with DHS, the committee electronically issued its Interim Report (reproduced as Appendix J in this final report). Subsequently the committee received the full DHS (2006) report documenting the analysis in the BTRA of 2006. While DHS agreed with the recommendations of the Interim Report and planned to address them, the committee did not learn of any progress up to the conclusion of its deliberations in May 2007 that would obviate those recommendations, which require sustained work.
>
> However, the content of the DHS (2006) report and information gained at additional meetings with DHS and national experts have significantly changed the committee's overall assessment of the BTRA of 2006. The committee identified errors in mathematics, risk assessment modeling, computing, presentation, and other weaknesses in the BTRA of 2006. It recommends against using this current BTRA for bioterrorism risk assessment as presented in the BTRA of 2006 or proposed for 2008. Instead, the committee offers improvements that can significantly simplify and improve future risk assessments. The improved BTRA should be used for risk management as well as risk assessment, as intended by HSPD-10.

1.3 Resistance to Change

Despite the profound critique offered by the NRC (representing its constituent members from the National Academy of Sciences and its sub-groups, the National Academy of Engineering and the Institute of Medicine), the Department of Homeland Security appears to remain committed to the methodology originally developed for BTRA 2006. Anecdotally, some of this surprising approach can be credited to "push-back" from the laboratories tasked with specific pieces of BTRA development. In a more formal sense, this kind of behavior has been well studied in the national security

and psychological literature (Allison and Zelikow; Janis, Jervis, Lebow and Stine; Lebow and Stine) and represents a combination of resistance at the laboratory or working level as well as a preference among policy makers for various simplified forms of intelligence as well as a profound reliance on standard operating procedures as well as decisional heuristics which rely on the familiar and apply cognitive principles of matching to the most familiar alternative.

Although the NRC critique has only been partially accepted by DHS, and there are a number of methodological flaws which remain to be addressed in DHS treatment of bioterrorism (and which should clearly NOT be extended into present and future models of nuclear terrorism)

It is nonetheless worthwhile to review the most significant flaws of BTRA 2006. In addition to an excessively complex treatment of probability improperly abstracted from the standard quantum mechanical treatment of probability (for a complete discussion of the theoretical probabilities of quantum mechanics see Northrop, 1979) BTRA 2006 is flawed in several other significant ways. The following section explains some of the problems of DHS' approach and suggests a more rigorous methodology for dealing with bioterrorist threats.

2.1 Intelligent Adversary Risk Analysis

The DHS BTRA 2006 treated terrorist attacks largely in the manner of uncertain hazardous events, rather than actions by an intelligent adversary. The methodology employed, Probabilistic Risk Assessment Event Trees, consists of a sequence of random variables, called events or nodes. The probabilistic event tree nodes are then loosely coupled to a consequence analysis.

As the NRC report indicates:

> Each random-event branching node is followed by the possible random-variable realizations, called outcomes, or arcs, with each arc leading from the branching, predecessor node, to the next, successor-event node (and it can be said without ambiguity that the predecessor event selects this outcome, or, equivalently, selects the successor event). With the exception of the first event, or root node, each event is connected by exactly one outcome of a preceding event. A node with no successor event is called a final event, or leaf. From each event, it is possible to trace a unique path back through alternating predecessor outcomes and events to the root event. The path from the root to a particular leaf is called a scenario. Each successive random event in a scenario path has a probability depending on all preceding outcomes in the path, and the probability of this scenario is the joint probability of the intersection of the outcomes on the path and is the product of these outcome probabilities. A natural way to construct an event tree is to place events in the chronological order in which they occur, if this order is known (e.g., Paté-Cornell, 1984).

> In practice in the BTRA, the event tree is not actually evaluated as shown in Figure 3.4; each of the 28 agents (outcomes of events in Stage 3) is analyzed in isolation, yielding 28 sets of, in theory, as many as 350 million paths based on as few as 5,448 distinct probabilities for each agent.
> Although the maximum number of possible scenario paths is large (i.e., exponential in problem size), agent-by-agent, the event tree has many paths terminated early with no attack (e.g., by failure to manufacture an agent, by successful interdiction, and so on), while others continue to completion. Among the 28 event trees, each corresponding to the selection of a different agent, DHS (2006) reports one agent with only 1,184 scenarios, and another, the largest agent tree, with
> 192,928 scenarios. The individual agent results are merged a posteriori into a distribution using probabilities for the selection of each agent and target. With the exception of this separation of event trees by agent, BTRA treats each of these successive events in ascending order of the stage in which it occurs.

Not only does this read like the "vacuum state" problem in string theory, but it also prescribes a methodology which is fundamentally wrong for the problem. Terrorist attacks are not random, but are purposive, require large organizational commitments (the postulated anthrax attack is more than an order of magnitude larger than the 9/11 attack and would require considerable intelligence and operational resources, if not outright state sponsorship) and are carried out by intelligent adversaries acting and reacting to a dynamic landscape as well as to the counter-terrorism strategies of their opponents (Hoffman, 1999; Fellman and Wright, 2003). While probabilistic risk analysis models uncertain hazards using probability distributions for threats, vulnerabilities and consequences based on a statistical analysis of past events, the risk analysis of terrorist attacks is fundamentally different than that of uncertain natural disasters and requires a methodology which incorporates the response of an intelligent adversary to changing conditions as shown in Appendix I (Parnell, Smith and Moxley, 2009). In comparing the intelligent adversary approach, Parnell, Smith and Moxley demonstrate how event trees underestimate intelligent adversary risk by assigning random probabilities to events which are actually decision nodes and which should be modeled as a decision trees rather than event trees. In particular, they develop a canonical intelligent adversary risk model for homeland security which incorporates sequential attacker-defender decisions and outcomes (Appendix II).

The canonical intelligent adversary risk model has six components, the initial actions of the defender to acquire defensive capabilities, the attacker's uncertain acquisition of the implements of attack (e.g., agents A, B, and C), the attacker's target selection and method of attack(s) given implement of attack acquisition, the defender's risk mitigation actions given attack detection, the uncertain consequences, and the cost of the defender's actions. The model consists of three material elements – a decision analysis whether to increase the levels of vaccine, whether to add a city

to the BioWatch program and how to calculate the effects of a pathogen not detected by Biowatch:

> In our defender– attacker–defender decision analysis model, we have the two defender decisions (buy vaccine, add a Bio Watch city), the agent acquisition for the attacker is uncertain, the agent selection and target of attack is another decision, the consequences (fatalities and economic) are uncertain, the defender decision after attack to mitigate the maximum possible casualties, and the costs of defender decisions are known. The defender risk is defined as the probability of adverse consequences and is modeled using a multiobjective additive model similar to multiobjective value models. We have assumed that the defender minimizes the risk and the attacker maximizes the risk. We implemented this model as a decision tree (Fig. 3) and an influence diagram (Fig. 4) using DPL…

Figures three and four are identical to appendices I and II in the current paper. The mathematical formulation of the model is contained in appendix four. The model uses COTS software to quantitatively evaluate the potential risk reductions associated with different options and likewise uses COTS software to make cost-benefit decisions. The model then provides outputs with respect to both budget vs. risk as well as the cumulative distribution (Appendix III). Among the conclusions which the model demonstrates are that:

> …spending US$ 0 or US$ 10 million gives the defender a 10% chance of zero risk, whereas spending US$ 20 or US$ 30 million gives the defender an almost 50% chance of having zero risk. The best risk management result would be that option 4 deterministically or stochastically dominates (SD) option 3, option 3 SD option 2, and option 2 SD option 1. The first observation we note from Fig. 6 is that options 2, 3, and 4 stochastically dominate 1 because option 1 has a higher probability for each risk outcome. A second observation is that while option 4 SD option 3, option 4 does not SD option 2 because option 4 has a larger probability of yielding a risk level of 0.4. Along the x-axis, one can see the expected risk (ER) of each alternative. This expected risk corresponds to the expected value of risk from the budget versus risk rainbow diagram. This example illustrates a possibly important relationship necessary for understanding and communicating how the budget might affect the defender's risk and choice of options.
>
> Risk managers can run a value of control or value of correlation diagram to see which nodes most directly affect the outcomes and which are correlated…Because we only have two uncertainty nodes in our canonical model, the results are not surprising.

> The graphs show that the ability to acquire the agent is positively correlated with the defender risk. As the probability of acquiring the agent increases, so does defender risk. In addition, the value of control shows the amount of risk that could be reduced given perfect control over each probabilistic node, and that it is clear that acquiring the agent would be the most important variable for risk managers to control.

Admittedly, this is a basic example, but with a more complex model, analysts could determine which nodes are positively or negatively correlated with risk and which uncertainties are most important. In a probabilistic model of this type, which measures intent, and incorporates feedbacks, the interesting feature of the model is the decision driven (i.e. strategic) step function as shown in appendices three and four. Because the core of the model is based on a Min/Max formulation, the stochastically dominant step functions is a natural, if slightly counter-intuitive outcome. More detailed models can be developed with more extensive data about attacker intentions, but the gist of this model is that unlike the BTRA 2006 model, it provides concrete guidance and allows risk managers to peg a given decision to a given cost and expected value.

3.1 BioWar

BioWar is scalable city-wide simulation, capable of simultaneously simulating the impact of background diseases, natural outbreaks and bioterrorism attacks on the population's behavior within a city. The multi-agent simulator includes social and institutional networks, weather and climate conditions, and the physical, economical, technological, communication, health, and governmental infrastructures which modulate disease outbreaks and individual behavior.

Individual behaviors include health seeking, entertainment and work/school behavior. A wide variety of reports are generated based on user needs including absenteeism patterns, pharmaceutical purchases, Dr. office insurance claims reports, and ER reports. Sub-reports are available for specific sentinel groups including the military, first responders and health workers. All reports reflect actual reports that can be made available to analyst or public health personnel including the delays in generating said reports.

Currently the system has been used to model five metropolitan areas including Washington D.C., Norfolk, Pittsburgh, and San Diego. Each city is modeled using actual census, geographic, weather, school district, and business/entertainment location data. BioWar includes a symptom based disease model in which the symptoms displayed by the agent depends on their socio-demographic background and the progression of the disease. To date, 62 diseases have been modeled including smallpox and anthrax. BioWar also includes a self and physician diagnostic model. Agents can self diagnose on the basis of visible symptoms and so decide whether to stay home, purchase over-the counter drugs, or go the Dr's office or the emergency room. Physicians diagnose on the basis of those symptoms and can run tests useful in diagnosis. Note the diagnosis can be wrong. Attack models include aerosolize attacks

and people-as-disease-carriers. Finally, there are a few preventive and response features that can be turned on or off depending on the analysts need – including vaccination, alert of medical personnel, general alert, and alert of agents who were known to be at the site of the known attack.

Validation has been done with respect to weather and climate, social network, city layout, Physician and ER office visits, and the purchase of apx 6 broad categories of OTC drugs. Work is ongoing to create an automated validation and tuning tool and to increase level and type of validation. New reports are generated as needed for particular projects. Currently BioWar has been used to generate data to test detection routines for 5 different companies.

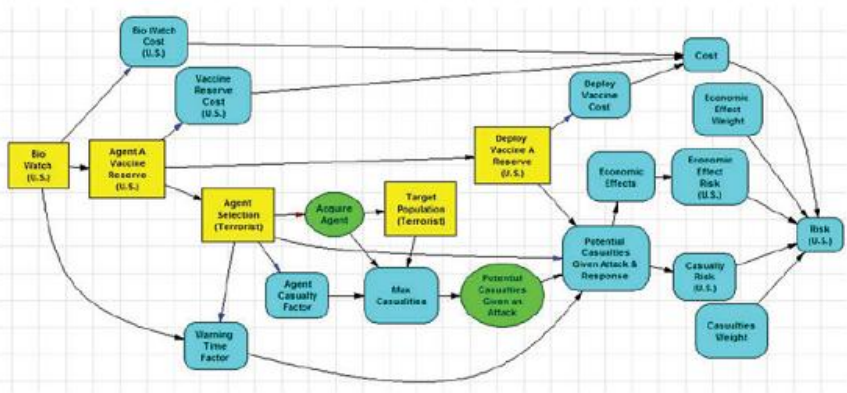
Planned extensions include increased fidelity of the disease model (e.g., increasing number to over 500 diseases) and communication model (mass media, and web-based information), first order models of other sensors such as tiger chips, water and air sensors, potential response models (such as quarantine, rapid drug disbursement (as with Cipro), and altered public information), additional attack models including water and food-borne attacks. We expect to continue to do optimization and validation as new features are added and new real data becomes available to us. Possible other extensions include linking to various GIS systems, infrastructure models, modules for military bases overseas, and to various real time data feeds. In addition, additional extensions as needed for DHS will be done.

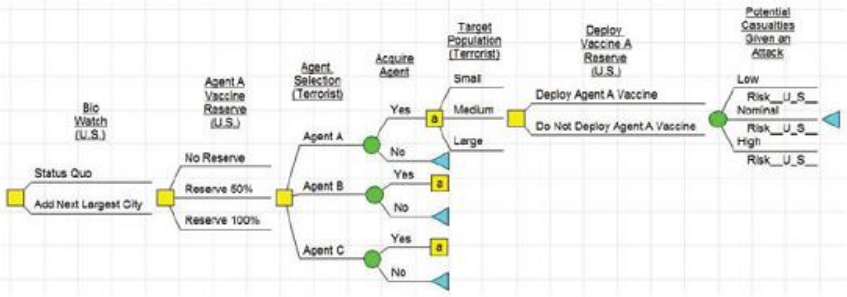
Appendix I: Probabilistic Risk Assessment vs. Intelligent Adversary Modeling[2]

	Uncertain Hazards	Intelligent Adversaries
Historical Data	*Some historical data:* A record exists of extreme events that have already occurred.	*Very limited historical data:* Events of September 11, 2001, were the first foreign terrorist attacks worldwide with such a huge concentration of victims and insured damages.
Risk of Occurrence	*Risk reasonably well defined:* Well-developed models exist for estimating risks based on historical data and experts' estimates.	*Considerable ambiguity of risk:* Adversaries can purposefully adapt their strategy (target, weapons, time) depending on their information on vulnerabilities. Attribution may be difficult (e.g. anthrax attacks).
Geographic Risk	*Specific areas at risk:* Some geographical areas are well known for being at risk (e.g., California for earthquakes or Florida for hurricanes).	*All areas at risk:* Some cities may be considered riskier than others (e.g., New York City, Washington), but terrorists may attack anywhere, any time.
Information	*Information sharing:* New scientific knowledge on natural hazards can be shared with all the stakeholders.	*Asymmetry of information:* Governments sometimes keep secret new information on terrorism for national security reasons.
Event Type	*Natural event:* To date, no one can influence the occurrence of an extreme natural event (e.g., an earthquake).	*Intelligent adversary events:* Governments may be able to influence terrorism (e.g., foreign policy; international cooperation; national and homeland security measures).
Preparedness and Prevention	Government and insureds can invest in well-known mitigation measures.	Attack methodologies and weapon types are numerous. Local agencies have limited resources to protect potentially numerous targets. Federal agencies may be in a better position to develop better offensive, defensive and response strategies.

[2] Taken from Parnell, Gregory S., Smith, Christopher M. and Moxley, Frederick I. (2009) Intelligent Adversary Risk Analysis: A Bioterrorism Risk Management Model, Society for Risk Analysis, DOI: 10.1111/j.1539-6924.2009.01319.x

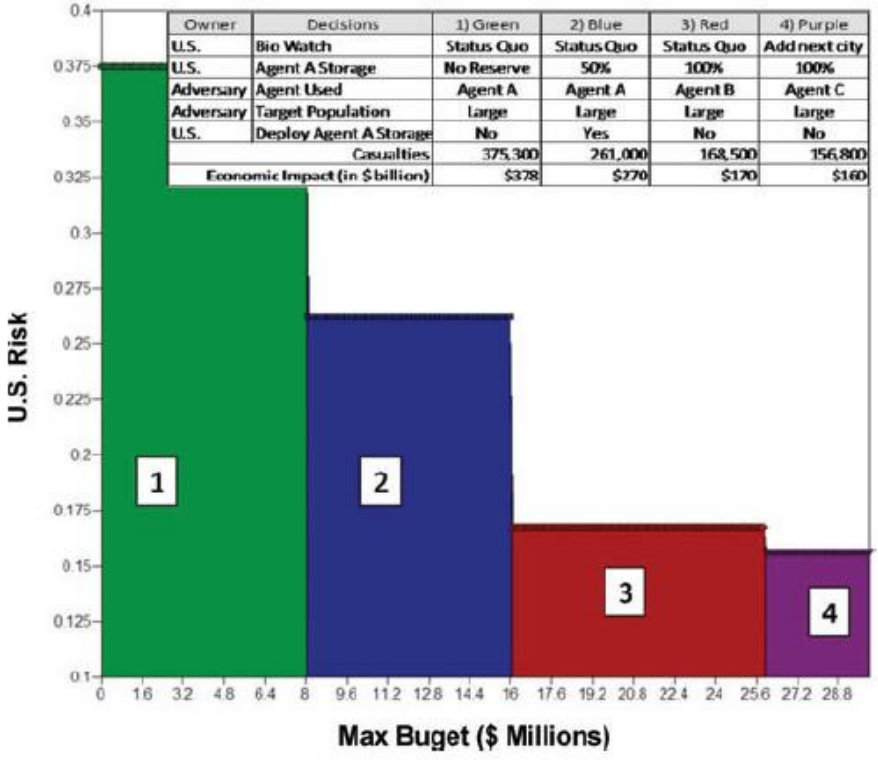
Appendix II: Canonical Intelligent Adversary Risk Management Model[3]



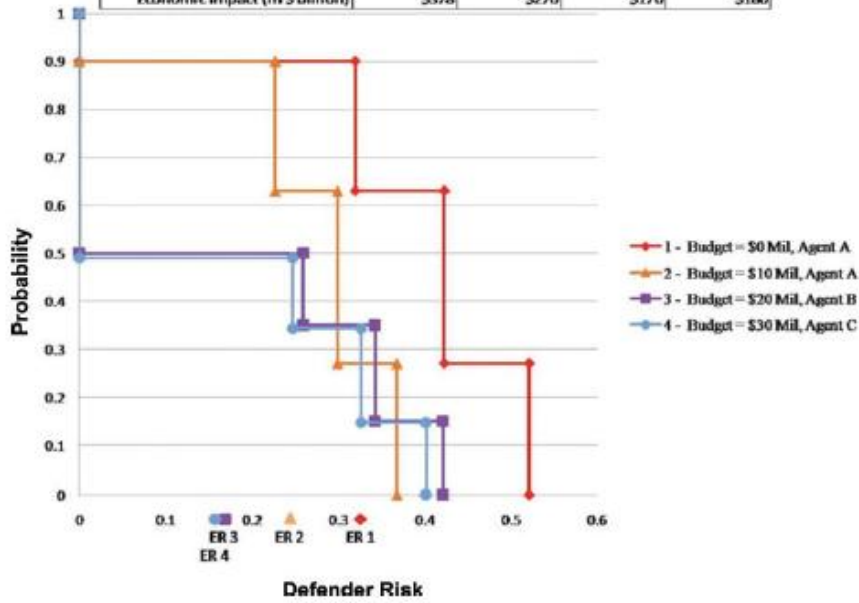


[3] Ibid.

Appendix III: Model Probability Distributions[4]



Owner	Decisions	1 Red	2 Orange	3 Purple	4 Blue
U.S.	Bio Watch	Status Quo	Status Quo	Status Quo	Add next city
U.S.	Agent A Storage	No Reserve	50%	100%	100%
Adversary	Agent Used	Agent A	Agent A	Agent B	Agent C
Adversary	Target Population	Large	Large	Large	Large
U.S.	Deploy Agent A Storage	No	Yes	No	No
	Casualties	375,300	261,000	168,500	156,800
	Economic Impact (in $ billion)	$378	$270	$170	$160



Complementary cumulative distribution.

[4] Ibid.

Bibliography

[1] Allison, Graham and Zelikow, Philip (1999) The Essence of Decision, Longman, 2nd edition, 1999

[2] Department of Homeland Security Bioterrorism Risk Assessment: A Call for Change, Committee on Methodological Improvements to the Department of Homeland Security's Biological Agent Risk Analysis, National Research Council, ISBN: 0-309-12029-2, http://www.nap.edu/catalog/12206.html

[3] DHS (Department of Homeland Security). 2006. Bioterrorism Risk Assessment. Biological Threat Characterization Center of the National Biodefense Analysis and Countermeasures Center. Fort Detrick, Md.

[4] Fellman, Philip V., and Wright, Roxana (2003) "Modeling Terrorist Networks: Complex Systems at the Midrange, London School of Economics, Joint Complexity Conference, http://www.psych.lse.ac.uk/complexity/Conference/FellmanWright.pdf

[5] Fellman, Philip V., (2011) "The Complexity of Terrorist Networks" International Journal of Networking and Virtual Organisations, (IJNVO), Vol. 8, Issue 1-2, Inderscience, 2011

[6] Fellman, Philip V., (2011) "The Complexity of Intelligence Estimates", Proceedings of the 8th International Conference on Complex Systems, New England Complex Systems Institute, Quincy MA, June, 2011

[7] Interim Report on Methodological Improvements to the Department of Homeland Security's Biological Agent Risk Analysis, Committee on Methodological Improvements to the

[8] Department of Homeland Security's Biological Agent Risk Analysis, National Research Council, ISBN: 0-309-66957-X, http://www.nap.edu/catalog/11836.html

[9] Hoffman, Bruce (1999) Inside Terrorism, Columbia University Press

[10] Janis, Irving (1982) Groupthink: Psychological Studies of Policy Decisions and Fiascoes, Houghton Mifflin

[11] Jervis, R., Lebow. N, and Stein, J (1989) Psychology and Deterrence (Perspectives on Security), Johns Hopkins University Press

[12] Jervis, Robert; Lebow, R. N., and Stein, Janis (1989) Psychology and Deterrence: Perspectives on Security, Johns Hopkins University Press

[13] Lebow, R. N. (1981) Between Peace and War, Johns Hopkins University Press, 1981

[14] Lebow, R.N, and Stein, Janis (1994) We All Lost the Cold War, Princeton Studies in International History and Politics

[15] Merrick, Jason and Parnell, Gregory S. (2011) A Comparative Analysis of PRA and Intelligent Adversary

[16] Methods for Counterterrorism Risk Management, Society for Risk Analysis, DOI: 10.1111/j.1539-6924.2011.01590.x

[17] Northrop, F.S.C. (1979) The Logic of the Science and the Humanities, Greenwood Press Reprint

[18] Office of Homeland Security. 2002. National Strategy for Homeland Security. http://www.dhs.gov/xlibrary/assets/nat_strat_hls.pdf.

[19] Parnell, Gregory S., Smith, Christopher M. and Moxley, Frederick I. (2009) Intelligent Adversary Risk Analysis: A Bioterrorism Risk Management Model, Society for Risk Analysis, DOI: 10.1111/j.1539-6924.2009.01319.x
[20] The White House (2004) Homeland Security Presidential Directive 10 [HSPD-10]: Biodefense for the 21st Century. http://www.fas.org/irp/offdocs/nspd/hspd-10.html
[21] The White House (2007) Homeland Security Presidential Directive 18 [HSPD-18]: Medical Countermeasures Against Weapons of Mass Destruction http://www.fas.org/irp/offdocs/nspd/hspd-18.html