Risk Identification, Assessment, and Management for the 2006 Virginia Gubernatorial Inauguration

Anna Capetanakis, Brett D. Dickey, Courtney A. Harmer, Mark J. Orsi, Doug D. Stewart, *University of Virginia Capstone Team*

Abstract— **The ability to prevent, respond to, and recover from terrorist attacks as well as natural disasters is critical to national security. Successful preparation requires the coordination of many different agencies (local, state, federal, non-governmental and volunteer) in order to obtain optimal utilization of their available resources and capabilities. Currently, there is no standard system for collaboration between agencies to perform risk analysis. In addition, devising a methodology for choosing between various security options can be difficult and typically results in autocratic decision-making. These problems hinder the breadth and depth of contingency planning and should be addressed in order to increase the effectiveness of risk management applications.**

After the attacks that took place on September 11th, 2001, risk management has become a major concern for the United States. The President and CEO of ANSER Institute for Homeland Security says that the nation needs an "ongoing process that includes imagining attack scenarios, drafting strategies that span the cycle of national objectives, and independent gaming to test the efficacy of strategies…our nation's capacity for innovation…will yield increasingly robust national strategies" [3]. These recommendations outline the intent of the collaborative Adaptive Multiplayer Hierarchical Holographic Modeling (AMP-HHM) tool.

As a case study, the Capstone Team, in conjunction with the University of Virginia Center for Risk Management of Engineering Systems (CRMES), deployed the AMP-HHM tool for the 2006 Virginia Gubernatorial Inauguration. The AMP-HHM framework takes a holistic approach by providing a methodology for identifying most, if not all, of the entities of a system. This allowed participants in the risk analysis process to effectively identify risks associated with the inauguration. They then used this database of scenarios to assess the criticality of each risk in terms of likelihood and consequences. Based on a vast collection of assessments, the threats that posed the largest magnitude of risk were given priority. To mitigate these risks, a multitude of security options were brainstormed and then analyzed to determine which options should be implemented, based on their effectiveness, cost, and consequences.

After the risk analysis process was completed, five threat scenarios were selected as the focus for evaluating policy options. It was determined that nine broad security categories could be employed to address the five selected threats. From these security options, four were determined to be superior: security guards, fire prevention, networking, and the fortification of surrounding infrastructures. These results were used by the Office of Commonwealth Preparedness (OCP) to better prevent, prepare for, and respond to catastrophic events through increased awareness and more efficient allocation of resources (personnel, security devices, etc.). The inauguration exercise provided insight on the effectiveness of the AMP-HHM tool as a risk analysis aid. The lessons learned from this exercise are being used to improve the software in order to increase its effectiveness in contingency planning for future risk analysis applications, such as the 2007 Jamestown Anniversary.

I. Introduction

A. *What is the problem?*

For any public event, such as the Virginia Gubernatorial Inauguration, government agencies and private volunteer organizations face the daunting task of planning for any risk – whether it be catastrophic or minor. Currently, there is no coherent, collaborative system in place to evaluate different risk scenarios. This lack of communication leads to the underutilization of experience specific to each organization. Each party will have knowledge that may be relevant to the planning activities of other organizations. In addition, it is often difficult to analyze the effectiveness of feasible security options because they are highly situational and decisions are made on an ad hoc basis. Ultimately, the security countermeasures that are put in place do not take into consideration the views of many relevant experts; instead, they usually depend on the experience and instinct of one person or a small committee.

B. *Why is the problem important?*

A large crowd of spectators is an attractive target for terrorists. The substantial increase in traffic flow and change in the community dynamic (different store hours, cancelled events, etc.) may open up opportunities for terrorists to strike. The presence of a large group of people, most of them likely unfamiliar with the territory, leads to the potential for mass panic and loss of life. It is imperative that government agencies be able to evaluate the most important risk scenarios and mitigate those risks as effectively as possible, based on thorough research and analysis according to the combined expertise of all preventive agencies involved. The Homeland Security Council recently "developed fifteen all-hazards planning scenarios for use in national, federal, state, and local homeland security preparedness activities" as a framework for risk management applications [9]. This project goes a step further by generating threat scenarios specific to each deployment (e.g., event, infrastructure), increasing the effectiveness of risk management.

C. *What has been done so far and by whom?*

In the past, risk scenarios would be generated through person-to-person brainstorming sessions, and there was not a standard way to evaluate the scenarios or a communal repository. Furthermore, varying security options were rarely systematically explored in terms of effectiveness, cost, and consequence.

The CRMES has been developing the Adaptive Multi-Player Hierarchical Holographic Model (AMP-HHM) since 2002. This tool, based on the *Groove* software platform, works toward facilitating better collaboration among multiple organizations that are planning security for the same event. The CRMES has been working to refine the tool, and through test bed applications, promote its use by government agencies.

II. Goals and Objectives

A. *Project objectives*

Through the application of risk analysis concepts and tools, the project aims to:

1) Develop an extensive HHM that encompasses multiple perspectives
2) Create a risk management plan for the OCP that:
    a) Minimizes all threats to the inauguration
    b) Organizes and prepare first responders in the event of a tragedy by effectively and efficiently allocating needed resources (personnel and critical resources)
3) Identify possible policy options to address the critical threat scenarios identified in the HHM
4) Analyze policy options
    a) Use the metrics "loss of lives," "economic damage," and "cost of implementation" to compare policy options
    b) Contact users who participated in the AMP-HHM game for the inauguration to obtain expert opinions
5) Analyze the performance of the AMP-HHM tool and further enhance the software by making recommendations for improved functionality

B. *Deliverables*

The Capstone Team provided a risk analysis framework for the collaborative generation and assessment of risk scenarios to prioritize critical threats. A risk management plan for the top ten threat scenarios was delivered to the Office of Commonwealth Preparedness (OCP). This plan was the basis for developing policy options to address each scenario. A thorough analysis of nine identified policy options was conducted to determine the effectiveness of each option on five selected threat scenarios.

III. Alternatives

A. *The baseline alternative*

One default alternative to this project would be to simply apply minimal uncoordinated effort to secure the event. However, this would leave the event susceptible to attacks and also ensure that any catastrophe would be magnified by poor recovery ability. This alternative was unacceptable because it put the life of the governor and the public at high risk, not to mention the potential damage to historical buildings and surrounding critical facilities.

B. *Proposed solution*

Contingency planning should be based on a database of potential threats and their corresponding likelihoods and consequences. After identifying the potential threats, select the policy option(s) that reduce the number of lives lost and/or the economic damage. Collect data through the use of the AMP-HHM tool, and choose the policy option that will minimize casualties/economic damage, based on expert elicitation and a review of related literature.

C. *Other alternatives*

There are a few other methods to attempt to ensure the safety of an event; however, none of them are as effective or efficient as the proposed solution. The following alternatives are presented in the order of most to least effective.

One alternative is data collection through face-to-face meetings. This would ultimately create results similar to ours, but will take much more time, will require more extensive scheduling, and does not allow for as many participants. Additionally, some threat scenarios may be omitted and some information may be unknown at the time of the meeting.

Another alternative is to increase security without a formal risk management plan. This is an ad hoc approach and will help to increase security, but it minimally addresses the issue of recovery time in the event of an attack. This method fails to address all possible scenarios. Many risk scenarios will undoubtedly be omitted without formal planning for the event.

Thus, each alternative has certain benefits, but none offer the holistic planning of the proposed solution.

IV. Evaluation Criteria

The research project has multiple evaluation criteria. The first depends on the *participation rate* of the agencies involved. The agencies identify threat scenarios which become the data on which the risk management plan is based. If the participants are not actively involved, the risk management plan will be limited. More data leads to a more thorough plan. Also, more data are a sign of an active and complete brainstorming session, giving confidence that all possible threat scenarios have been considered.

Another evaluation criterion is the *number* of agencies involved in creating this risk management plan. A greater number increases the validity of the results because there are more diverse opinions.

A less vital evaluation criterion is to determine the effectiveness of the plan. This can be done by analyzing the outcome of the event and comparing it to the risk scenarios that had been created. If any incidents occurred, the ranking of those scenarios will be evaluated. Low rankings will be analyzed to identify why the assessments were incorrect. [

The final criterion is to evaluate the effectiveness of the AMP-HHM tool and also devise a systemic method for adapting it for other similar future events. This will require surveying the participants and determining any improvements that may contribute to the wide-scale acceptance of the software. This will more than likely include: error-proofing, minimizing loading times, improving ease-of-use, and adding any functionality to the tool that could increase its usability. Additionally, this project aims to generalize the methodology for applying the AMP-HHM tool to any similar event. Devising a methodology that is robust, resilient, and redundant is essential to securing public events.

V. Major Project Activities and Expected Results

A. 2006 Virginia Gubernatorial Inauguration

In order to create an extensive HHM that encompasses multiple perspectives, various government agencies (Virginia Department Of Transportation, Virginia Department of Emergency Management, Department of Homeland Security, local police and fire departments, and others.) with relevant expertise must be involved to carry out the identification, assessment, and management of risk. The Capstone Team recruited members from these agencies to participate in the risk analysis process, which was performed through the use of the AMP-HHM tool. The Capstone Team then distributed compact disc copies of the tool to the participants and provided technical support for the installation. Once this was done, the team split participants into three teams for the duration of the AMP-HHM game: Red, Blue 1, and Blue 2. The Red Team represented the terrorist group perspective, using only publicly known information to identify vulnerabilities that can be exploited. The blue teams, however, used a wider set of information that they had available, including classified information within their agencies. They represented the counter-terrorist group**.** The teams created three HHMs (or workspaces). After the agency teams created a large collection of potential risks, the Capstone Team merged all of the HHMs into one integrated model for the next stage, risk assessment. During this phase, users entered their judgments on the likeliness of each risk and how severe the consequences might be. This resulted in a set of assessments that implied the level of danger each risk posed. This concluded the development of the HHM, which was the first major project milestone.

After ranking the risks according to their assessments, the Capstone Team called a meeting to discuss contingency planning that was implemented to mitigate the most critical risks. This meeting allowed participants to brainstorm precautionary measures and develop a safe, effective plan of action based on the results of the AMP-HHM tool. This plan sought not only to minimize threats to the inauguration, but also to better prepare first responders in the event of a catastrophe. Finally, the Capstone Team presented the risk management plan to our client, the Virginia Governor's Office of Commonwealth Preparedness.

B. Risk Management Policy Option Evaluation

Following the inauguration, the Capstone Team performed an analysis of potential policy options which were or could have been implemented. They first sought to collect all possible options for minimizing potential risks. The team used two different sources of information: the risk management options that were developed for the Office of Commonwealth Preparedness, and visits to the site of the inauguration.

This effort produced fifty-three potential policy options. Analyzing each of these would be too large a project to be feasible. Therefore, to narrow these options, the team clustered similar options into more generalized policies. For instance, security guards patrolling the event, security guards monitoring the perimeter, and others were grouped into one category called "security guards." For each clustered option, experts were interviewed to determine the most reasonable and effective method of organizing each cluster. For example, police chiefs were interviewed to find out how they would deploy security guards for an event such as the inauguration. In addition, the team asked each expert to give their estimate of the damage that would be caused by each risk scenario. This was represented by a triangular distribution of lives lost, economic damage, and the efficacy rate of each policy option. The damage estimate was also represented by a triangular distribution plus the cost for implementing their suggested method, or option.

The team then utilized Monte Carlo simulation to determine the distribution and expected values of the lives lost and economic damage for each policy option. This provided data for comparing options to determine tradeoffs between cost and lives lost and economic damage. These comparisons also allowed the team to eliminate inferior solutions and identify a Pareto-optimal decision set.

VI. Results and Discussion

The game finished with 289 identified risk scenarios and 77 assessed scenarios. Figure 1 displays the distribution of the 77 assessed scenarios. This was more than enough threat topics to provide sufficient analysis and recommendations for the OCP.

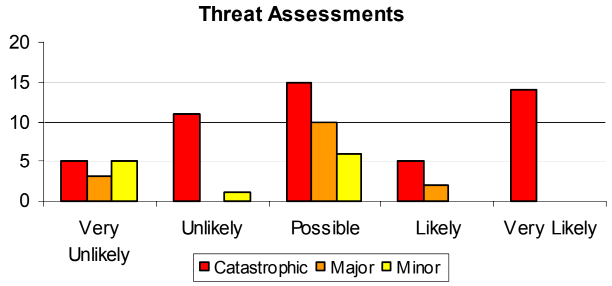

Figure 1: Breakdown of Assessment Results.

The risk scenarios were first ranked using primarily the consequences and then the likelihoods (for example, a scenario with high consequences and low likelihood would be ranked ahead of a scenario with low consequences and high likelihood). When more than one player assessed a threat, the assessments that had the most catastrophic and/or greatest likelihoods were used for the analysis. The members of these agencies brainstormed potential threat scenarios using HHMs, and then assessed those threats based on likelihood and consequences.

A. Findings

Below is a summary of all of the threat topics that were determined to be the biggest risks to the inauguration.

1) **Arson Attack –** Setting fire to the historic buildings that immediately surround the inauguration. This included explosions and explosive devices in the utility tunnels below Williamsburg.
2) **Sniper Attack –** Shooting at people from an anonymous location without the victims' knowledge.
3) **Biological Attack** – Using viruses, toxins, or bacteria to intentionally harm a targeted group of people (e.g., nerve agent).
4) **Chemical Attack –** Delivering a harmful chemical to the event via airplane, explosive, or other method**.**
5) **Rocket-Propelled Grenade Attack –** Firing an explosive weapon that can be launched from a range of 500-1000 meters.

For each individual threat scenario, security options were proposed in order to best secure the inauguration. Security options from all scenarios were considered. Similar options were clustered to produce a more manageable number, and the following security options were selected:

1) **Security Guards** – Deploying guards to sweep, secure, and parole the immediate area of the event.
2) **Bio/Chemical Weapon Technology** – Utilizing technology to detect biological and chemical weapons.
3) **Fire Prevention** – Using firefighters, fire trucks, and other associated countermeasures to prevent and combat fire.
4) **Networking** – Having open communication between involved agencies and between agencies and the public.
5) **Entrance Scans** – Using metal detectors and security personnel to scan vehicles and attendees entering the event.
6) **On-site EMS teams** – Having Emergency Medical Service teams available on-site during the event.
7) **Increase Airport Security** – Alerting local airports to enhance security prior to the event.
8) **Fortification of Surrounding Structures** – Sweeping and securing buildings adjacent to the event.
9) **Aerial Monitoring/Support** – Deploying aircraft to survey the event.

B. Analysis

The nine security options were evaluated based on two metrics: the potential loss of life and the potential economic damage. These options were analyzed to determine the expected and conditional expected values (extreme case) of both metrics in the event of a threat scenario occurring where those options were implemented. This is displayed in Figures 3 and 4. Figure 2 is the legend for the security options shown in Figures 3, 4, 5, and 6.

A	**Security Guards**
B	**Bio/Chem Weapon Technology**
C	**Fire Prevention**
D	**Networking**
E	**Entrance Scans (Vehicle/Personnel/Attendees)**
F	**On-site EMS Response Teams**
G	**Increase Airport Security**
H	**Fortification of Surrounding Structures**
I	**Aerial Monitoring/Support**

Figure 2: Legend of Security Options

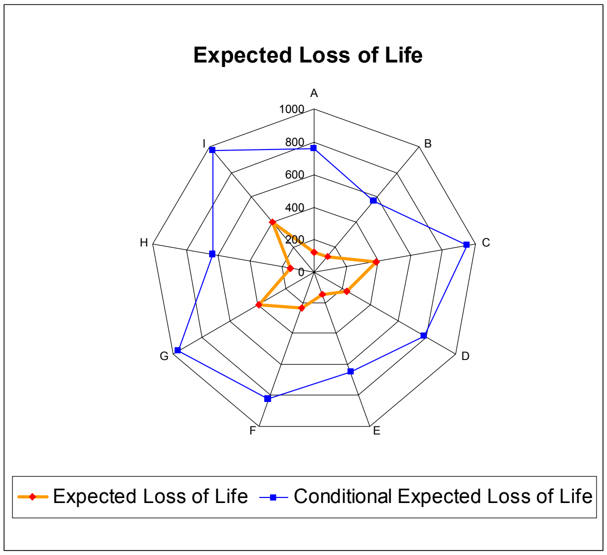

Figure 3: Loss of Life with Security Options

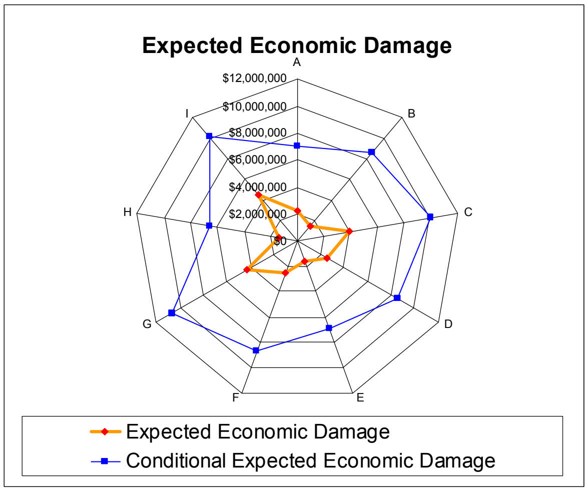

Figure 4: Economic Damage with Security Options

Based on loss of life, five options were considered to be Pareto optimal. These are displayed in Figure 5.

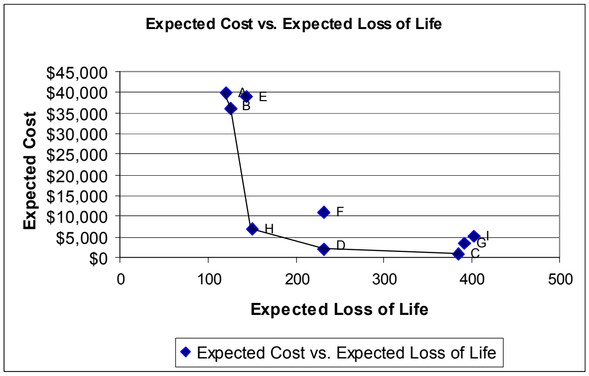

Figure 5: Pareto-Optimal Security Options Based on Loss of Life

Based on economic damage, four options were considered to be Pareto optimal. These are displayed in Figure 6. The Pareto-optimal results for both metrics identified four of the same security options. These were Security Guards, Fire Prevention, Networking, and Fortification of Surrounding Structures. A fifth security option was found to be Pareto optimal in only the loss-of-life metric (Figure 5). This option was Bio/Chem Weapon Technology.

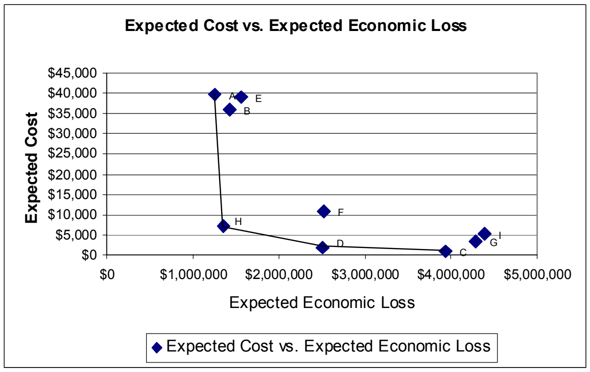

Figure 6: Pareto-Optimal Security Options Based on Economic Damage

C. Problems

When dealing with the players, the Capstone Team encountered multiple problems that were associated with motivation, communication, game-rule clarification, and computer literacy. These problems are listed below:

- Initially it was difficult to gain player participation.
- Players added excessive details to the HHM (i.e., the HHM should have only three tiers, and all the details are to be placed in the description window).
- Some players did not know how to use the tool or some of its functions.
- Players were vague when writing their comments/descriptions.
- Some players performed risk assessments based on personal biases instead of their technical expertise.

Fortunately, there were multiple face-to-face meetings throughout the game, so the Capstone Team was able to minimize these problems. During these meetings, the players were informed of current problems and how to avoid them. In these meetings it was also helpful to have the players express problems that they were experiencing with the AMP-HHM tool; this enabled identifying improvements to the current version. Some of these problems are listed below:

- When they closed out of *Groove,* some players were not able to save the work that they had added to the workspaces.
- Multiple players as well as Capstone Team members experienced problems installing *Groove.*
- Because the game was started with a very detailed HHM skeleton, players initially were not motivated to go through the HHM to see what already existed.
- The number of risk assessment levels was changed during the game, but the changes were not reflected within the software. This led to some confusion among the players.

Finally, problems were also encountered during the analysis of the results. The general problem was that the numbers used for the analysis were hard to come by and had a large uncertainty. Experts were consulted, but even they were unsure about certain measurements. The numbers that were hard to determine are listed below:

- The cost of implementing the policy options
- The possible loss of lives and the economic loss for each of the threat scenarios
- The effectiveness of a policy option for a specific threat scenario
- The details of policy options

VII. Conclusion

The purpose of this capstone was to create a risk management plan for the OCP in order to secure the 2006 Virginia Gubernatorial Inauguration against extreme events. The project was successful in identifying risks and creating a risk management plan for the OCP with numerous security options. The analysis performed on security options provided a further exploration of securing the inauguration. Analysis was done to determine the effectiveness of the tool in the development of a risk management plan. Additionally, we created a methodology for choosing security options that can be adapted for similar events. Since the Inaugural Ceremonies passed without any significant incident, an analysis was done on the effectiveness of the overall risk management plan.

Various agencies were brought together and performed a risk assessment for the inauguration. They were asked to do so using the AMP-HHM tool provided. The Capstone Team ranked the assessed threat scenarios. Those with the highest likelihood and consequences were placed at the top. The top risk scenarios were presented to the agencies in charge of security at the inauguration. With a risk management plan, the agencies could focus their time and effort on preventing the threats that would have the most adverse consequences. When the top threat scenarios were identified, security options for each were proposed. Experts evaluated the effectiveness of the various security options, which were used to determine superior and inferior options based on further analysis.

A. Implications

Based on the experience of this year-long project, the Capstone Team realized several implications:

- Collaborative risk analysis based on expert opinion is highly effective.
- Subjective interpretations and measurements can create difficulties and should be reduced as much as possible to prevent autocratic decision-making.
- Risk management as a field of study is fairly new and requires further research and development.

B. Future Work

The methodologies used in this project can be repeated for other risk management applications, such as Jamestown's 2007 Anniversary. Other areas that require additional research are:

- Further development of the AMP-HHM tool
- Loss of information during mergers
- Quantitative ranking system for assessed topics
- Accepted methodology to evaluate security options

ACKNOWLEDGMENTS

The 2005-2006 University of Virginia Capstone Team 10 would like to acknowledge the following people and organizations for their contributions to this project:

Sponsor: The Office of Commonwealth Preparedness

Organizations Participating in AMP-HHM: Virginia Department of Transportation, Virginia Department of Emergency Management, Department of Homeland Security, Department of Aviation, Federal Highway Administration, Charlottesville Fire Department, Arlington Police Department

University of Virginia Faculty and Students: Yacov Haimes, Joost Santos, Barry Horowitz, James Lambert, Abhinav Agrawal, Mark Waller, Paul Zelinke, Zhenyu Yan, Oliver Mills, Steve McHail

REFERENCES

[1] Apostolakis, G. & D.Lemon. (2005) A screening methodology for the identification and ranking of infrastructure vulnerabilities due to terrorism. *Risk Analysis* 25(2). 361-376.

[2] Center for Risk Management of Engineering Systems. (2005) *Adaptive Two-Player Hierarchical Holographic Modeling (ATP-HHM).* University of Virginia, Charlottesville, VA.

[3] David, R. (2002). *Homeland Security: Building a National Strategy.* National Academy of Engineering. Retrieved April 3, 2006 from the World Wide Web: http://www.nae.edu/nae/bridgecom.nsf/weblinks/CGOZ-58NLJY?OpenDocument.

[4] Haimes, Y. (2005). *Deployment of the Adaptive Multiplayer HHM Game for the 2006 Virginia Gubernatorial Inauguration.* SEAS Proposal No. SE-VTRC-2683-06.

[5] Haimes, Y. & B. Horowitz. (2004a). Adaptive two-player hierarchical holographic modeling game for counterterrorism intelligence analysis. *Journal of Homeland Security and Emergency Management* 1(3).

[6] Haimes, Y. & B. Horowitz. (2004b). Modeling interdependent infrastructures for sustainable counterterrorism. *Journal of Infrastructure Systems,* 33-42.

[7] Haimes, Y. (1998). *Risk Modeling, Assessment, and Management.* New York: John Wiley & Sons, Inc.

[8] Horowitz, B. & Y. Haimes. (2003). Risk-based methodology for scenario tracking, intelligence gathering, and analysis for countering terrorism. *Systems Engineering* 6(3). 152-169.

[9] Howe, D. (2004). *Homeland Security Council: Planning Scenarios.* Retrieved April 3, 2006 from the World Wide Web: http://www.voiceoffreedom.com/archives/homelandsecurity/15-attacks_the_hawiaa_disclosure.htm.

[10] Lambert, J., Y. Haimes, D. Li, R. Schooff, & V. Tulsiani. (2001). Identification, ranking, and management of risks in a major system acquisition. *Reliability Engineering & System Safety* 72(3). 315-325.

[11] Lamm, G. & Y. Haimes. (2002). Assessing and managing risks to information assurance: a methodological approach. *Systems Engineering* 5(4). 286-314.

[12] Leung, M., J. Lambert, & A. Mosenthal. (2004) A risk-based approach to setting priorities in protecting bridges against terrorist attacks. (2004). *Risk Analysis* 24(4). 963-984.

[13] Major, J. *Advanced Techniques for Modeling Terrorism Risk.* National Bureau of Economic Research Insurance Group Conference. Retrieved October 19, 2005 from the World Wide Web: http://www.guycarp.com/pdf/major_terrorism.pdf

[14] NRC (National Research Council). (2002). *Making the Nation Safer: The Role of Science and Technology in Countering Terrorism.* Washington, DC: The National Academies Press.

[15] Oster, C. (2002, April 8). Can the risk of terrorism be calculated by insurers? game theory might do it. *Wallstreet Journal Online.* Retrieved October 19, 2005 from the World Wide Web: www.gametheory.net/news/Items/011.html

[16] Santos, J. & Y. Haimes. (2004). Modeling the demand reduction input-output (I-O) inoperability due to terrorism of interconnected infrastructures. *Risk Analysis* 24(6). 1437-1451.