ABSTRACT

The paper develops a methodology for analyzing risk to the meat supply, with a specific focus on slaughterhouses. The safety of the nation’s meat supply from terrorist attack has become a major concern of the USDA after the September 11th attacks on the Pentagon and World Trade Center. The methodology performs a risk assessment through Hierarchical Holographic Modeling (HHM). The goal of the HHM is to capture all observables of a terrorist attack as well as identify all of the vulnerabilities of the target. A 2-player game using a Blue Team and Red Team aided in completing a more thorough HHM diagram. This process identified key observables such as researching of toxins and access to meat processing machines as possible indicators of an attack. Bayes’ Theorem serves as the key tool for analyzing the observables identified through the HHM diagram to assess the likelihood of terrorist attack.

1 INTRODUCTION

Terrorism is not a new problem, yet only in recent years have American intelligence and security agencies devoted significant resources to terrorism studies. Modern terrorism originated in the 1960’s, and since that time has changed dramatically, “in ways that make it more dangerous and difficult to counter. International terrorism once threatened Americans only when they were outside the country. Today international terrorists attack us on our own soil” (National Commission on Terrorism). The deaths and destruction terrorists have inflicted worldwide is both sobering and horrifying; “terrorist organizations have become the cancer of free nations” (Herren 1). Recent directions in terrorism are disturbing, including trends “toward loosely organized, self-financed, international networks of terrorists, . . . terrorism that is religiously- or ideologically- motivated, . . . growth of cross-national links among different terrorist organizations” (Lee). More frightening than any of these, however, is the noticeable and deliberate trend toward the development, capture, and use of weapons of mass destruction (WMD). Terrorism will continue to be a serious strategic and tactical threat throughout this decade, as this new terrorism “does not confine itself to any boundaries and possesses a terrifying lethality” (Whine 6). Attacks like those on the World Trade Center and the Pentagon, or the Washington D.C. sniper, will become even more commonplace without increased intelligence collection resources and new methods of analysis.

The threat from terrorism extends far beyond traditional attack scopes; the nation’s food supply is one system that only recently has been considered a viable target. The potential impact of a terrorist attack using biological or chemical agents is enormous; thousands could be killed or made ill, hundreds of millions of dollars could be lost, and millions would be subjected to intense fear and anguish. With this threat in mind, the United States Department of Agriculture seeks a way to assess and manage risks to the food production process. Working with Professors Yacov Haimes and Barry Horowitz, the Capstone team has developed an adaptable and robust methodology that gives America’s intelligence and security agencies a new weapon in the war on terror. Incorporating modeling techniques and quantitative analysis, this framework allows for better visualization and assessment of the complexities and relationships within the terrorism system. Through the implementation of this methodology, the disruption, fear, destruction, and death caused by acts of terror can be mitigated.
2 METHODOLOGY

2.1 General HHM

Formulating a complete framework that fully models and analyzes systems this complex and dynamic is implausible if not impossible; the Capstone project strives to present a basis that can be expanded and integrated with current data collection and analysis techniques. The fundamental theory behind the framework is that of employing systems analysis and risk analysis techniques in the study of terrorism. Through the incorporation of risk, modeling terrorist networks becomes an invaluable tool to visualize and describe the system. Hierarchical Holographic Modeling (HHM) is introduced as a modeling approach that has already achieved success with defense and civilian infrastructure systems and has great potential in capturing the complexities and interconnectedness present in terrorist network systems.

Hierarchical Holographic Modeling reflects a significant departure from earlier modeling schemas. “The name is suggested by holography – the technique of lensless photography. The difference between holography and conventional photography . . . is analogous to the difference we see between conventional mathematical modeling techniques . . . and the hierarchical holographic modeling schema” (Haimes, Risk Modeling, 97). This technique has the capability to be more successful than previously applied models because of its dynamic characteristics. As stated by Haimes et al:

The HHM methodology/philosophy is grounded on the premise that in the process of modeling large-scale and complex systems, more than one mathematical or conceptual model is likely to emerge. Each of these models may adopt a specific point of view, yet all may be regarded as acceptable representations of the infrastructure system. Through HHM, multiple models can be developed and coordinated to capture the essence of the many dimensions, visions, and perspectives of infrastructure systems. (385)

The model is the basis for understanding the different state variables and the interactions or causal relationships between them.

For the Capstone project, an HHM of terrorist acts on the food production process was formulated from the Blue Team’s perspective. Head topics were considered covering a broad range of potential observables, including mode of attack, location and security of the target, current intelligence, and potential impacts. Subtopics were then determined that represent the range of possibilities for each head topic; this provides the basis for scenario creation and filtering. Considering the system from the defender’s perspective initially allowed for greater emphasis on the factors the Capstone Team felt would be most important to the owner of a facility, including security, employment practice, and cleanliness. To create a more complete model, attacks from the terrorists’ perspective were also considered, resulting in more head and subtopics that were incorporated into the Blue Team’s HHM. Initially general attacks were considered, and then broken down into specific attacks on various stages of the food production process, for example a slaughterhouse, processing facility, or distributor.

The HHM approach allows for continual updates on head topics and subtopics by experts as new factors characterizing terrorism and the food production process are discovered. The purpose of the model is to serve as the first stage of an extensive risk assessment process. From the HHM, a set of risk scenarios can be created using variations within each subtopic, “If done well, the set of scenarios at any level of the hierarchy approach a ‘complete set’” (Horowitz, “Countering” 8). Risk in this context indicates the possibility of a terrorist attack. Given the enormous number of all potentially constructed scenarios, the methodology strives to filter and rank these scenarios based on the likelihood of occurrence and estimated impacts.

2.2 Red Team Exercise

Prevention of terrorist activity, although never guaranteed, involves further understanding of a terrorist’s intentions and thought processes. In response to this finding, the Capstone team conducted a Two-Player Hierarchical Holographic Modeling (HHM)-game experiment. The purpose of the experiment was to extract the expert’s opinion, in this case the terrorism, so that the threat of terrorism could be best addressed from an additional perspective. Posing as terrorists, the participants first used HHM to identify the sources of risk related to attacking a slaughterhouse; and then developed detailed attack plans using the general HHM models as a basis.

2.2.1 Experimental Setup and Objectives

The game consisted of two teams of participants commonly referred to as “Red Teams”, each consisting of three undergraduate students. Each participant was instructed to think and act as terrorists so that information could be gathered from a terrorist’s perspective. The conductors of the experiment (Capstone team) were concerned with the terrorist’s general thought processes, final decisions, and the reasoning behind both. The terrorist teams were responsible for completing two tasks: (1) organize all possible factors that contribute to the execution of a terrorist at-

Florentine, Isenstein, Libet, Neece, Zeng, Haimes, and Horowitz
tack on a slaughterhouse using Hierarchical Holographic Modeling (HHM), and (2) formulate a specific attack plan that targets activities of the production process within a specified slaughterhouse.

2.2.2 Task 1: Data Gathering Using Hierarchical Holographic Modeling

Hierarchical Holographic Modeling, a risk-modeling tool, was the method used for recording the participant’s thoughts. Following a brief tutorial on HHM, the participants began to brainstorm all the observable factors associated with an attack on a slaughterhouse. The students organized and recorded their thoughts using the HHM methodology. In order to further understand the concept and importance of HHM as a risk modeling tool, a section of the model developed by a Red Team is described in the next paragraph.

In developing the model, the method of contamination was identified as a critical component in an attack plan and was therefore created into a head topic. With the head topic chosen, the next step was to determine the specific aspects of this category otherwise known as subtopics. Similar to the head topics, the use of each of the subtopics in a final plan would have to be observed. Examples of sub topics included within “Contamination Method” were water supply and pipeline. Figure 1 below is the entire Contamination Method portion of the general HHM model.

![Contamination Method Diagram]

Figure 1: Limited HHM for Attack on Slaughterhouse

2.2.3 Task 2: Data Gathering Through Role-playing

The scenario portion of the experiment is a continuation of the initial task of constructing general hierarchical holographic models. More specifically, having already developed a general framework consisting of all the factors related to attacking a slaughterhouse, the teams then drew from the head topics and sub topics to design an attack plan. The Red Teams were instructed to formulate a detailed attack plan on the United State’s food supply targeting a fictional slaughterhouse in Hardin, Montana. To assist the participants in accessing related information, the Capstone team also created a fictitious website to accompany the facility. For reliability and repeatability purposes, each team was given the same resources, which included internet access as well as the conductors of the experiment. If information other than that provided via the website was desired, the experimental subjects could ask any of the facilitators to answer a question from the perspective of a specific role. Each subject had to identify the person they believed could best address the question, and include the means used to contact that person.

This type of role-playing described above best simulates the actions of a real terrorist during the structuring of an attack. In order to further understand the observable events of terrorist scenarios, the potential attack is divided into six stages (see Table 1). Even though the scenarios developed by the Red Teams touched on all six divisions, the setup and focus of the analysis section of the paper was on observing the planning and preparing stages of an attack.

<table>
<thead>
<tr>
<th>Stage</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Intent</td>
<td>This is the earliest stage, where the terrorist develops malice and an intent to harm via a general attack plan.</td>
</tr>
<tr>
<td>Target Acquisition</td>
<td>At this stage, the terrorist chooses specific target(s).</td>
</tr>
<tr>
<td>Plan</td>
<td>The terrorist researches the target(s) and curious attack options.</td>
</tr>
<tr>
<td>Preparation</td>
<td>This is a full commitment stage. At this point, the wheels are in motion as the terrorist prepares to launch the attack.</td>
</tr>
<tr>
<td>Execution</td>
<td>The attack is carried out.</td>
</tr>
<tr>
<td>Grace Period</td>
<td>Depending on the nature of the attack, there is sometimes a time-lag between a successful attack and its impact. For example, poisoning food does not result in harm until someone eats the food.</td>
</tr>
</tbody>
</table>

Table 1: Six Stages for Identifying Observable Terrorist Scenarios [Horowitz and Haimes 2003:16]
3 COMBINED HHM ANALYSIS

Once the Red and Blue teams completed their analysis on the given scenario and created HHM models, the next phase was to compare the various models. This was done to determine the amount of knowledge or information that was gained from using multiple perspectives when examining a terrorist scenario.

The first part of the comparison method involved the creation of a combined Hierarchical Holographic Model, based on both Red and Blue Team models. The combined model was used to visually describe the similarities and differences in the information created by each group. To show the process of merging and to preserve the lineage of each variable a color-coded system was used.

Primary analysis compared the original Blue Team model to the combined model and returned the increase in the amount of information. Secondary analysis of the HHM models focused on the amount, if any, of important information gained from using the combined model rather than that of the Blue Team alone. This portion of the analysis made use of the likelihood given to each head/sub-topic by the Red Teams. The likelihood of each subtopic was given three values by each Red Team: lowest, expected, and highest. These three values were then used to find the triangular distribution of the event using the formula:

\[ E[X_a] = \frac{(a + b + c)}{3} \]

Where \( a \) is the highest value, \( b \) is the expected, and \( c \) is the lowest. This outputs a single likelihood value for each subtopic.

This phase of the analysis focuses on the 119 variables that were included in the combined HHM model, but not in the Blue Team model. The five most important variables considered were those included in both Red Team models, but not in the Blue Team model. The initial trial run of the experiment has shown that multiple perspective analysis outputs a more complete model than single perspective analysis. The Blue Team missed a substantial amount of information, and much of this was considered of extreme importance by the Red Teams. This information can be used to increase the knowledge of the Blue Team and form a more complete model.

4 ANALYSIS OF THREAT

Once proper intelligence has been gathered, it must be analyzed to determine whether or not it indicates a threat to a slaughterhouse. The information must be deemed reliable before any action can be taken on the intelligence. Also, the information should indicate at a high level of likelihood that a terrorist attack is going to take place. Another important consideration is the interaction of multiple sources and pieces of intelligence in improving both the credibility of the information and the likelihood of an attack taking place.

4.1 Credibility of Information

In order to begin the analysis of information, one must first determine the credibility of the information being used. The use of historical data and false positives/negatives provide the information necessary to determine the credibility of information. Professor Barry Horowitz has been working to develop the method to perform the analysis using Bayesian Theory. To do the actual calculations, first define the following variables:

<table>
<thead>
<tr>
<th>Definitions of Variables</th>
</tr>
</thead>
<tbody>
<tr>
<td>( P(T) ) = Probability reported action is taking place</td>
</tr>
<tr>
<td>( P(T) ) = Probability reported action is not taking place</td>
</tr>
<tr>
<td>( P(T</td>
</tr>
<tr>
<td>( P(T</td>
</tr>
<tr>
<td>( P(A</td>
</tr>
<tr>
<td>( P(A</td>
</tr>
</tbody>
</table>

The fact that the action is taking place in this case does not necessarily mean that the information is indicative of a terrorist attack. At this point the information is only being verified for correctness, later it will be used to determine the likelihood of an attack.

Using these variables, analysts are interested in \( P(T | A) \) as this indicates the likelihood the information is correct. \( P(T | A) \) can be calculated using Bayes’ Theorem as follows:

<table>
<thead>
<tr>
<th>Equations</th>
</tr>
</thead>
<tbody>
<tr>
<td>( P(T</td>
</tr>
<tr>
<td>( P(T</td>
</tr>
</tbody>
</table>
The exact numbers for the variables may be difficult to calculate; however, the most important aspect of the equation is the ratio between the variables. For an action that is not common (the type of action analysts would be most interested in examining) the ratio \( \frac{P(T)}{P(T)} \) would be large. The ratio \( \frac{P(A \mid \overline{T})}{P(A \mid T)} \) must be small in order to counteract the first ratio being large. If this ratio is exactly one, then the information provides no information of value. The ratio being larger than one provides information that the probability the action is taking is place is actually reduced. The smaller the second ratio is, which is the relationship between receiving the information when the action is not being taken over receiving the information when action is being taken, the more credible the information. Law enforcement officials then can decide at what level of credibility they would act on the information.

4.2 Confirmation Through Second Source

Additional information may confirm or challenge a previous assumption. The first set of equations shows how multiple sources of information may be combined to gain a better assessment of the credibility of the information. The relationship of the sources may range from perfectly independent to perfectly correlated. Perfectly independent means that the information gained from one source does not influence the information gained from the other source. Perfectly correlated means that the first source completely influences the second source to the point the information is actually identical. In reality, most sources fall somewhere in between these two extremes.

The first section addresses perfectly independent sources. To solve this problem, the variables become:

<table>
<thead>
<tr>
<th>Definitions of Variables</th>
</tr>
</thead>
<tbody>
<tr>
<td>( P(T \mid A) ) = Probability source A is true</td>
</tr>
<tr>
<td>( P(T \mid \overline{A}) ) = Probability source A is false</td>
</tr>
<tr>
<td>( P(T \mid B) ) = Probability source B is true</td>
</tr>
<tr>
<td>( P(T \mid \overline{B}) ) = Probability source B is false</td>
</tr>
<tr>
<td>( P(T \mid A,\text{and},B) ) = Probability sources are true when A and B agree</td>
</tr>
<tr>
<td>( P(T \mid A,\text{and},\overline{B}) ) = Probability sources are false when A and B agree</td>
</tr>
</tbody>
</table>

Assuming independence of sources A and B, the equations to calculate \( P(T \mid A\,\text{and}\,B) \) are as follows:

<table>
<thead>
<tr>
<th>Equations</th>
</tr>
</thead>
<tbody>
<tr>
<td>( P(T \mid A) = 1 - P(T \mid A) )</td>
</tr>
<tr>
<td>( P(T \mid B) = 1 - P(T \mid B) )</td>
</tr>
<tr>
<td>( P(T \mid A,\text{and},B) = 1 - P(T \mid A)P(T \mid B) )</td>
</tr>
</tbody>
</table>

These equations provide a very simplified expression for the calculation of the improvement of the credibility of information. The first two equations calculate the probabilities of no attacks given evidence A or B. The third equation then uses the prior calculations to calculate the probability of an attack by subtracting the probability no attack would occur given both A and B and subtracting this probability from one. This calculation is the upper limit however on the improvement on the credibility since it assumes independence between the sources. In reality though, at least a small amount of correlation usually exists between sources and in many cases the sources may be highly correlated. The true combined credibility would fall somewhere between the highest of the credibilities of A and B and the credibility calculated for independent sources. A numerical example of this analysis is as follows:

<table>
<thead>
<tr>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>( P(T \mid A) = .6 )</td>
</tr>
<tr>
<td>( P(T \mid B) = .3 )</td>
</tr>
<tr>
<td>( P(T \mid A) = 1 - .6 = .4 )</td>
</tr>
<tr>
<td>( P(T \mid B) = 1 - .3 = .7 )</td>
</tr>
<tr>
<td>( P(T \mid A,\text{and},B) = 1 - .4 \times .7 = .72 )</td>
</tr>
<tr>
<td>( \text{Max Credibility} = .72 )</td>
</tr>
<tr>
<td>( \text{Min Credibility} = \text{Max (Credibility A, Credibility B)} = .6 )</td>
</tr>
<tr>
<td>( \text{Range}: .6 &lt; \text{Credibility Of A and B} &lt; .72 )</td>
</tr>
</tbody>
</table>

In the above example, the original credibility of the data was .6. An additional piece of data appeared that had a credibility of .3. Using the formula assuming independence of the information, the new level of confidence became .72. This serves as the maximum credibility. Since the credibility of one piece of information cannot be weakened by information that agrees, the minimum new level of confidence is .6. This provides a range for the confidence with the true value being closer to .6 for highly correlated sources and closer to .72 for highly independent sources.
4.3 Likelihood of an Attack

Once the information is deemed credible, an evaluation of the likelihood of an attack must be completed. Four critical observables of a slaughterhouse labeled \( A, P, IF, \) and \( IA \) are defined below. The only primary assumption for analysis was that there was no known prior information.

For the Bayesian analysis, let:

\[
\begin{align*}
T &= \text{an individual is intending on committing an attack on a slaughterhouse} \\
\overline{T} &= \text{an individual is not intending on committing an attack on a slaughterhouse} \\
A &= \text{this individual has gained access to a slaughterhouse} \\
P &= \text{this individual has acquired a type of poison or harmful agent.} \\
IF &= \text{this individual has sought information on slaughterhouses and has been caught.} \\
IA &= \text{this individual has sought information on poisons or other harmful agents and has been caught.}
\end{align*}
\]

The following probability values pertain:

\[
\begin{align*}
p(T) &= .00000001 \\
p(\overline{T}) &= 0.99999999 \\
p(A \mid T) &= .999 \\
p(A \mid \overline{T}) &= .000001 \\
p(P \mid T, A) &= .6 \\
p(P \mid \overline{T}, A) &= .0001 \\
p(IF \mid T, P, A) &= .6 \\
p(IF \mid \overline{T}, P, A) &= .4 \\
p(IA \mid T, IF, P, A) &= .8 \\
p(IA \mid \overline{T}, IF, P, A) &= .2
\end{align*}
\]

These probabilities were derived from assessments of the Red Team’s input as well as the Capstone Team’s background research. Note \( p(T) \) is rather small, but \( p(A \mid T) = .999 \) is large.

Using Bayesian analysis,

\[
p(T \mid A) = \frac{p(A \mid T)p(T)}{p(A \mid T)p(T) + p(A \mid \overline{T})p(\overline{T})}
\]

Substituting the assessed values yields that \( p(T \mid A) = 0.009891187 \).

Now consider the case where it is known an individual has both a toxic agent and gained access to the facility, and we want the probability of a terrorist attack conditional on those two:

\[
p(T \mid P, A) = \frac{p(T \mid A)p(P \mid T)}{p(T \mid A)p(P \mid T) + p(P \mid T)p(\overline{T})}
\]

Substituting the example values yields \( p(T \mid P, A) = 0.983590417 \). This value is a factor almost ten million times greater than the likelihood without information.

Similarly, it can be shown that \( p(T \mid IF, P, A) = 0.98900011 \) and \( p(T \mid IA, IF, P, A) = 0.997227152 \). Note that the posterior probability values remain relatively constant after the first two signals were observed. Comparatively, the value gained by observing an individual researching slaughterhouse facilities and harmful agents was not significant. Both events provided only increased probability by factors of one.

4.3.1 Individual Signals

The evaluation of each signal independent of the others makes use of the same observables and corresponding probability values described above. In addition, as noted previously, the only assumption was that there was no known prior information.

Using Bayesian analysis,

\[
p(T \mid A) = \frac{p(A \mid T)p(T)}{p(A \mid T)p(T) + p(A \mid \overline{T})p(\overline{T})}
\]

Substituting the assessed values yields that \( p(T \mid A) = 0.009891187 \). The knowledge that this individual has gained access to a slaughterhouse results in a value almost one million times greater than the likelihood without information.

Continuing with the Bayesian analysis,

\[
p(T \mid P) = \frac{p(P \mid T)p(T)}{p(P \mid T)p(T) + p(P \mid \overline{T})p(\overline{T})}
\]

This equation is determining the likelihood of a terrorist intending to commit an attack on a slaughterhouse, given that this individual has acquired a poison or harmful agent. Substituting the example values yields \( p(T \mid P) = 0.0000599964 \). This value is a factor almost six thousand times greater than the likelihood without information.

Similarly, it can be shown that \( p(T \mid IF) = 0.000000015 \) and \( p(T \mid IA) = 0.0000004 \).
The value of knowing that this individual has researched slaughterhouse facilities increased the probability by a factor of 1.5. Finally, if the intelligence community caught this individual seeking information on poisons or other harmful agents the probability increases by a factor of four.

4.4 Analysis of Results

Applying Bayesian analysis provided a quantitative basis for helping the intelligence community understand how the quality of individual data items based on specific scenarios of concern relate to improvements in the overall system performance. It also illustrated how to determine which signal among many is the most valuable to collect. In summary, it demonstrated the importance of information in assessing terrorist threats before they become a reality.

4.4.1 Interpretation of Results

4.4.1.1 Multiple Signals

Evidently, the criteria used for ranking the signals affected the results of the evaluation. Based on the sequencing of the factors, the information gained from observing $IF$ and $IA$ was not of particular significance. This was because the value of information gained from $IF$ and $IA$ was accounted for in the first two observable events. In other words, $IF$ and $IA$ are not independent of $A$ and $P$. A terrorist intending to commit an attack on a slaughterhouse that has already gained access and acquired a poison would most likely have engaged in prior research related to events $A$ and $P$. However, if the sequence was reorganized so that $IF$ and $IA$ were the initial observations, they would provide a greater value of information. The first two events of interest, $A$ and $P$, would then be dependent on $IF$ and $IA$.

The analysis also proved the value of considering multiple pieces of information. The likelihood of an individual intending to commit an attack increases by a factor of ten million if it is known that an individual has previously gained access to a slaughterhouse. An increase of this magnitude emphasizes the importance of this single piece of data. However, knowledge of the second event of interest, poison acquisition, increased the initial likelihood by a factor of 100 million. This suggests that by tracking and obtaining one additional piece of information related to an attack on a slaughterhouse, the chances of confirming an attack is 100 times greater than if only the first factor was observed. Even though the third and fourth events ($IF$ and $IA$) were dependent on the first two factors ($A$ and $P$) they still managed to increase the likelihood of determining an individual’s intentions on committing an attack on a slaughterhouse.

4.4.1.2 Individual Signals

As illustrated above, the criterion used to sequence the signals has an affect on the results of the Bayesian analysis. To compensate for this influence, each signal can be evaluated independently of the others. By assessing each signal individually, intelligence agencies have a quantitative measure of how valuable each observable is in determining the overall likelihood of a terrorist intending to commit an attack on a slaughterhouse. This type of analysis is particularly useful when resources are limited and the government has to decide on select signals to track.

The signals deemed most valuable to track are those that increase the probability of a terrorist intending to commit an attack on a slaughterhouse $P(T)$, most substantially. The results of the analysis suggest that the order in which the signals should be targeted and subsequently examined is: $A, P, IA, IF$. The results indicate that a terrorist has the greatest intentions of attacking a slaughterhouse if they have gained access to the facility, and least likely when having performed general research on slaughterhouses. Investigating slaughterhouses is less suspicious than researching poisons when all the agricultural, academic, and scientific environments that study animal facilities are considered.

4.4.2 Limitations

The criteria used to sequence the observable events directly impacts the results of the Bayesian analysis. As illustrated in the case above, the first piece of information (access to a slaughterhouse) dramatically increased the likelihood of the person’s intention to commit an attack. The value of this information was clear by the magnitude of which the probability increases. However, it is important to note that there may be circumstances that prevent one from obtaining this piece of information. For example, there may be confusion as to who is responsible (federal, state, or local agencies) for collecting the information, thus neglecting to ever obtain the piece of intelligence. In such a case, intelligence agencies might choose to rely more heavily on other observables or even opt to change the criteria for ranking the events. Lastly, in addition to the criteria for analysis, the scenario to which the methodology is applied will affect the increase in likelihood.

5 CONCLUSIONS

The 2P-HHM Methodology is a sound method based on previous risk analysis techniques. It can be applied to a variety of scenarios, without change to its fundamental ideology. The method is an easily adaptable way to evaluate the risks that face a system. An important aspect of the method is that not only is information acquired from a va-
riety of sources, but also the importance of each variable is included in the model.

The initial run of the methodology has outputted a model that describes the risks that face a slaughterhouse. These risks, the factors that may cause the risk, and critical pieces of intelligence are all included in the model. These items can be used to increase the security of a slaughterhouse, to improve the intelligence collection at the local and federal level, and to identify holes in the analysis of a single team.

The statistical analysis provides a method for resolving the issues of credibility of the source as well as updating the likelihood of an attack. These formulas do not take into account contradicting information, but this can be completed in a similar method as the confirming data. The value of the updates in the credibility and the likelihood will hopefully encourage the sharing of intelligence information.

REFERENCES


AUTHOR BIOGRAPHIES

CHRISTOPHER M. FLORENTINE is in the Systems and Information Engineering Department at the University of Virginia. His research interests include systems analysis and risk analysis. He enjoys sports, music, and playing guitar. He can be contacted by email at cmf5v@virginia.edu

MINDY L. ISENSTEIN is in the Systems and Information Engineering Department at the University of Virginia. Her research interests include modeling games and Bayesian analysis. She enjoys the theater, travel, and acting. She can be contacted by email at mli5a@virginia.edu

JARED Q. LIBET is in the Systems and Information Engineering Department at the University of Virginia. His research interests include statistical modeling, risk analysis, and terrorism network analysis. He enjoys tennis, backpacking, and card games. He can be contacted by email at jql3r@virginia.edu

STEVEN R. NEECE is in the Systems and Information Engineering Department at the University of Virginia. His research interests include risk analysis and Bayesian theory. He enjoys sports, movies, and officiating. He can be contacted by email at srn3e@virginia.edu

JIM S. ZENG is in the Systems and Information Engineering Department at the University of Virginia. His research interests include modeling games, Bayesian analysis, and software development. He enjoys candlelit dinners and long walks on the beach. He can be contacted by email at zeng@virginia.edu