Abstract — Expert knowledge is vital in assessing security risk. An Expert’s perception is based on his knowledge and experience. Experts involved in security risk assessment from different domains might perceive risk from different perspectives. Their opinions are valuable sources of knowledge which can be analyzed with statistical tools to assess security risks. This paper illustrates an analysis of expert’s judgment in the maritime domain. Spearman’s rank correlation coefficient was calculated to determine the degree of correlation of experts from the same expert group.

Keywords - Expert Knowledge, Delphi Method, Security Risk Assessment

I. RISK AND RISK MANAGEMENT

Risks exist in almost all aspects of life. Individuals and organizations alike must decide how to reduce risks. Grimaldi and Simonds prioritized five activities in decreasing effectiveness for reducing risks as follows [1]:

1. Eliminate hazard
2. Guard against hazard
3. Warn against hazard
4. Training
5. Personal protective equipments

Many hazards cannot be eliminated. For example, human beings know no way to prevent most natural disasters effectively, such as hurricanes, tornadoes, earthquakes, etc. We have been unable to eliminate all terrorist acts and all human errors. Consequently in many cases we eliminate what we can and then guard against the hazards that cannot be eliminated; for example building codes can be improved to guard against damages from earthquakes or hurricanes. Human factor design principles and control systems can be installed to guard against human errors. Warning systems can be used to guard against hazards. For example, on-coming trains blow their whistles, certain products carry warning labels, and high voltage signs appear on the voltage junction boxes.


The risk management cycle involves five stages: identify, assess, plan, mitigate, and control. The most important and challenging stage of the cycle is risk assessment. Many organizations from different parts of the world are working diligently to understand the basic components of risk and to come up with different methodologies to control or mitigate risk.

Maritime risk and safety analysis must include the probabilities of unwanted and/or unavoidable maritime incidents or “events” and their consequences.

Risk from natural disasters includes category III, IV, or V hurricanes, tropical storms, and other types of severe weather conditions (category: natural disasters). Man-made events contributing to maritime risk can be intentional or unintentional. Intentional events include sabotage and terrorism. Unintentional events include human error such as mental lapses and procedural errors and mechanical failures such as power plant, structural, or navigational errors. Each category has several linked incidents or “events” of occurrence and can cause disruption in the maritime domain. Maritime incidents can be categorized under the headings of collision, grounding, fire and explosion, pollution (major spills are mainly a result of the aforementioned three causes but can also result from human error).

The risks posed to maritime transport from the terrorist organizations include cargoes, vessels, facilities, people, and money. Some activities are linked with these elements that can pose security risks. For example, cargo can be used to smuggle people and/or weapons and to transport conventional, nuclear, and chemical, or biological weapons. Vessels can be used as a weapon to launch an attack (USS Cole-type act). Vessels can be attacked to cause human casualties. Vessels can be sunk in at strategic locations to disrupt shipping traffic. Terrorists can infiltrate by posing as seafarers [4].

Security related risk can be assessed by identifying internal and external threat scenarios linked with a particular event and negative consequences caused by that event. Charles Mitchell (ABSG Consulting) and Commander Chris Decker’s (U.S. Navy) paper, Applying Risk-based Decision-making Methods/Tools to U.S. Navy Antiterrorism Capabilities, highlights the importance of understanding the elements of “security risk” and its assessment [5].

Security Risk associated with an event can be expressed with the help of the traditional risk equation,

\[
\text{Risk} = \text{Probability(F)} \times \text{Consequence(C)}
\]

which is applicable to calculate risk associated with unintentional events. For intentional events which assumes an adversary, the Probability can be separated into two parts: threat and vulnerability and equation (1) is modified as,

\[
\text{Security Risk} = \frac{\text{[Threat(T) } \times \text{ Vulnerability(V)}]}{\text{ x Consequence}}
\]
The components of Security risk can be depicted in the Figure 1 below.

![Security Risk Diagram]

**Figure 1. Components of Security Risk**

“Threat” is a function of the attractiveness of a target. A particular situation can have multiple threat scenarios, and each scenario is very useful in the risk assessment stage. “Vulnerability” is susceptibility or weakness. Each threat scenario will have different levels of vulnerabilities depending on the safeguards provided for that particular situation or scenario. It is important to analyze the vulnerability for each threat scenario. “Consequence”, the third component, is the magnitude of the negative impact if an unwanted event occurs. Total risk is the sum of all risks taken over all possible events.

In this study we are concentrating on the risk associated with the maritime domain and concerned with the “events” that could disrupt shipping on the Sabine – Neches Waterway for a period of twenty-four hours or more. The ultimate goal of this study is to gather expert opinion to identify and prioritize likelihood of “events” on the Sabine – Neches waterway with the help of a panel of experts from this area and analyze their judgment on ranking these “events” from most likely (rank 1) to least likely (rank 10).

**II. RISK ASSESSMENT AND EXPERT OPINION**

Howard Kunreuther of the Wharton School, Center for Risk management, mentions some of the challenges in assessing, managing, and financing extreme events. His paper suggests the use of expert opinion in determining likelihood of attacks [6].

Dr. J.F. Bouchard suggests four methodologies for integrating threat, consequences, and vulnerability to conduct risk assessment [7]:

- Use quantitative data as much as possible, particularly for measuring consequences and vulnerability;
- Where subjective judgments must be applied, employ a panel of impartial subject matter experts to minimize the impact of personal biases and provide a broad range of expertise. The insurance industry, quite familiar with risk management and mitigation strategies, already employs this approach;
- Establish clearly-documented assessment and factor weighting criteria that allow risk assessments to be audited, thus ensuring the credibility of outcomes; and
- Put in place procedures to review and validate the data used in the risk assessment (including accuracy and credibility of sources), the analytical process itself (via review by outside experts in this type of analysis), and the outcomes (via a “red cell” or other body that thinks like an adversary and does a parallel assessment of weaknesses and potential scenarios).

United States Government Accountability Office’s report (GAO Report), Risk Management: Further Refinements Needed To Assess Risks and Prioritize Protective Measures at Ports and Other Critical Infrastructure offers recommendations for executive action: work with the intelligence community to develop ways to better assess terrorist threats and use available information and expert judgment to develop a relative probability for various terrorist scenarios and provide this information to sector-specific agencies [8].

Christine E. Wormuth’s paper, “Homeland Security Risk Assessment: Key Issues and Challenges”, states the importance of expert opinion in risk assessment. She claims, “Risk assessments – even if they are based on imperfect intelligence, expert opinion, and computer simulations of potential consequences – give us the tools to examine many different pieces of complex information in a structured way. They focus attention on the specific judgments that cumulate into an overall risk ranking and hence they can be “unpacked” to better understand where differences of opinion may lie and how they affect the assessment. Policy makers can use the structure that risk assessments provide to understand clearly where there are disagreements in the expert community, and can then assess for themselves the different sides of the debate before coming to a policy judgment that may have profound implications down the road.” She further emphasizes the importance and utilization of a national security risk assessment to strengthen homeland security policy development and resource allocation process [9].

**III. METHODOLOGY: DELPHI METHOD**

The Delphi Method is a structured process of data collection using the knowledge from a group of experts by means of a series of questionnaires. Subjective estimates from the experts are gathered, analyzed, and used as suitable information for decision making [10].

The method is structured on two important elements. The first element is anonymity among group members. This is required to encourage diverse opinions based on the expertise of each individual. The second element is controlled feedback in which the responses from the group members are gathered and summarized and then fed back to the group. Each panel member is asked to consider his/her responses in relation to the responses of the rest of the group. Based on this, they are asked to respond to the next round of the survey.

The method can be viewed as a controlled debate [11]. Extreme opinions from the group members are made open and clear via the controlled feedback, and estimates are achieved bypassing the problems of group dynamics.

The Delphi technique involves a series of questionnaires designed to gather a consensus of opinions. Linstone and Turoff’s book [10], *The Delphi Method: Techniques and Applications*, highlights the key properties of problems that might be approached via the Delphi technique. These properties are:

- The problem does not lend itself to precise analytical techniques but can benefit from subjective judgments on a collective basis;
- The individuals needed to contribute to the examination of a broad or complex problem have no history of adequate communication and may
represent diverse backgrounds with respect to experience or expertise;

- More individuals are needed than can effectively interact in a face-to-face exchange;
- Time and cost make frequent group meetings infeasible;
- The efficiency of face-to-face meetings can be increased by a supplemental group communication process;
- Disagreements among individuals are so severe or politically unpalatable that the communication process must be refereed and/or anonymity assured;
- The heterogeneity of the participants must be preserved to assure validity of the results, i.e., avoidance of domination by quantity or by strength of personality ("bandwagon effect") [10].

The Delphi Method can be implemented with the help of a ten-step procedure described by Fowles [12]:

1. Formation of a team to undertake and monitor a Delphi on a given subject.
2. Selection of one or more panels to participate in the exercise. Customarily, the panelists are experts in the area to be investigated.
3. Development of the first round Delphi questionnaire.
4. Testing the questionnaire for proper wording (e.g., ambiguities).
5. Transmission of the first questionnaire to the panelists.
7. Preparation of the second round questionnaire (and possible testing).
8. Transmission of the second round questionnaire to the panelists.
9. Analysis of the second round responses (Steps 7 to 9 are reiterated as long as desired or necessary to achieve stability in the results).
10. Preparation of a report by the analysis team to present the conclusions of the exercise.

Theodore J. Gordon’s paper “The Delphi Method” indicates that the selection of participants holds the key to a successful Delphi study [11]. Linstone and Turoff note that the potential users of the findings may be willing and useful members and their diversity of viewpoints that span respectable controversy will help to generate interest and involvement. The core strategy of Delphi study is to gather the collective judgments of experts [10].

The panel of experts used, to accomplish the project objective represented five core areas of the maritime domain. These areas, shown in Fig. 2, are public ports, the U.S. Coast Guard, the shipping industry, private ports/docks, and law enforcement.

Figure 2. The Delphi Project Panel of Experts

Two participants were selected from each of the five categories. The United States Coast Guard Port Arthur District, has authority over facilities and vessels on the Sabine–Neches Waterway. Therefore, the Coast Guard was contacted in order to define categories from which experts were to be chosen. Once these categories were agreed upon, the Coast Guard also helped to identify experts in each category.

The next important step in the Delphi project after selecting the panel of experts is to design the survey. Design of the questionnaires or the Delphi survey is based on the formulation of the problem statement or a question. These questionnaires are sent to the participants along with the additional information on the subject. The list of “events” generated for the project and Delphi survey is given below:

1. Major vessel accident causing waterway closure or disruption of vessel traffic for more than Twenty-four hours (unintentional, human error).
3. Port facility infrastructure breakdown (unintentional).
4. Damage to port facility, from a vessel equipment failure/malfunction (unintentional, navigational).
5. Terror threat (hoax) – causing shutdown of port facilities or parts of the Sabine–Neches Waterways.
6. Damage or destroy a large vessel or tanker with the help of a small vessel approaching it with explosives on board or by underwater improvised explosive devices (terrorist acts, USS Cole-type act).
7. Disruption of port facilities and/or operations by destroying key assets or infrastructure such as cranes, electrical power systems, etc. (intentional, terrorist acts).
9. Dense fog, coastal storms, hurricanes up to category II and other similar weather conditions (natural disaster).
10. Category III, IV, or V hurricanes (natural disaster).

The Delphi method is based on two or more round of surveys. After each round, survey data is analyzed and summarized and this information is fed back to the panel of experts.
Round 1:
(a) Provide a list of “events” that cause loss of life or negative economic impacts. Prioritize these “events” from most likely (Rank = 1) to least likely (Rank = 10) to occur in a calendar year.
(b) Each member of the panel may also suggest additional “events” to be considered.

Round 2:
Once the list of “Events” is generated from the first round, the research team will give feedback with the summary data and ask participants to reconsider their priorities.

They were given two weeks to complete the survey and return it by e-mail. Eighty percent (80%) of the participants returned the survey in the given time.

The findings of the Delphi project can be very useful in the overall process of risk management. It has special importance in terms of dealing with risks associated with extreme events dealing with terrorism [5].

IV. RESULTS

Survey rounds 1 and 2 achieved the desired objective of identifying and prioritizing events. Participants were requested to review and prioritize a list of events from most likely to least likely to occur in a calendar year and to suggest additional events to the original list. The results from round 1 of the survey were received by email or fax and summarized. The average, lowest, and highest priority ranking for each event was tabulated and provided to survey participants with instructions for round 2. In addition to the summary data from survey round 1, participants were given a round 2 survey form. In survey round 2, they were asked to reconsider their priority ranking and to provide a new priority ranking or reconfirm their original priority ranking.

The research team used SPEARMAN’S RANK CORRELATION COEFFICIENT to determine whether or not the rankings of the events by the two survey participants (SP1 and SP2) within groups (USCG, shipping industry, and private ports) are related [13] on both the survey rounds. We will determine the degree of positive or negative correlation between experts within each group. The experts were requested to rank these events from most likely to least likely to occur in a calendar year. Spearman’s rank correlation coefficient was used to measure the level of agreement among the experts within a group.

Eight experts from five groups were requested to rank ten events on the likelihood scale of 1 through 10. One member from group 1 (public ports) and one member from group 5 (law enforcement) did not return the survey. The participant from group 1 (public ports) was requested several times to complete the survey but did not reply. The participant from group 5 (law enforcement) opted out of the project because of security concerns. Spearman’s rank correlation coefficient was calculated for the agreement among panel members from group 2 (USCG), group 3 (shipping industry), and group 4 (private ports).

Table 1, 2, and 3 reflect the rankings of events by survey participants from USCG, shipping industry, and private ports group, respectively. Spearman’s rank correlation coefficients were used to calculate the correlations of rankings of events between the survey participants from group 2 (USCG) on both the survey rounds. The correlation coefficient for survey round 1, $r_{11}$ is 0.56, and for survey round 2, $r_{12}$ is 0.80. For group 3 (Shipping industry), the correlation of rankings of events between the survey participants for survey round 1 is $r_{21}$ is 0.921, and for survey round 2, $r_{22}$ is 0.951. The correlations of rankings of events between the survey participants from group 4 (private ports) for survey round 1, $r_{31}$ is 0.915 and for survey round 2, $r_{32}$ is 0.951.

Group 2 (USCG), Spearman’s Rank Correlation Coefficient:

$$r_{11} = 1 - \frac{6 \sum d^2}{n(n^2 - 1)} = 1 - \frac{6(72)}{10(99)} = 1 - \frac{432}{990} = 0.56$$

$$r_{12} = 1 - \frac{6 \sum d^2}{n(n^2 - 1)} = 1 - \frac{6(34)}{10(99)} = 1 - \frac{204}{990} = 0.80$$

Table 1 Rankings of events by survey participants 1, and 2 from Group 2, (USCG) for both the survey rounds.

<table>
<thead>
<tr>
<th>Event</th>
<th>Round 1 (R1)</th>
<th>Round 2 (R2)</th>
<th>Difference between Rank1 and Rank2</th>
<th>$d^2$</th>
</tr>
</thead>
<tbody>
<tr>
<td>SP1</td>
<td>SP2</td>
<td>SP1</td>
<td>SP2</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>2</td>
<td>3</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>2</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>3</td>
<td>8</td>
<td>3</td>
<td>5</td>
<td>3</td>
</tr>
<tr>
<td>4</td>
<td>5</td>
<td>4</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>5</td>
<td>9</td>
<td>9</td>
<td>-1</td>
<td>1</td>
</tr>
<tr>
<td>6</td>
<td>6</td>
<td>6</td>
<td>-1</td>
<td>0</td>
</tr>
<tr>
<td>7</td>
<td>7</td>
<td>8</td>
<td>-1</td>
<td>0</td>
</tr>
<tr>
<td>8</td>
<td>10</td>
<td>10</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>9</td>
<td>3</td>
<td>6</td>
<td>-3</td>
<td>0</td>
</tr>
<tr>
<td>10</td>
<td>4</td>
<td>7</td>
<td>-3</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>$\Sigma d^2 = 72$</td>
<td>34</td>
</tr>
</tbody>
</table>

Group 3 (shipping industry), Spearman’s Rank Correlation Coefficient:

$$r_{21} = 1 - \frac{6 \sum d^2}{n(n^2 - 1)} = 1 - \frac{6(13)}{10(99)} = 1 - \frac{78}{990} = 0.921$$

$$r_{22} = 1 - \frac{6 \sum d^2}{n(n^2 - 1)} = 1 - \frac{6(8)}{10(99)} = 1 - \frac{48}{990} = 0.951$$

Table 2 Rankings of events by survey participants 1, and 2 from Group 3, (shipping industry) for both the survey rounds.

<table>
<thead>
<tr>
<th>Event</th>
<th>Round 1 (R2)</th>
<th>Round 2 (R1)</th>
<th>Difference between Rank1 and Rank2</th>
<th>$d^2$</th>
</tr>
</thead>
<tbody>
<tr>
<td>SP1</td>
<td>SP2</td>
<td>SP1</td>
<td>SP2</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>4</td>
<td>-2</td>
<td>4</td>
</tr>
<tr>
<td>3</td>
<td>6</td>
<td>6</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>4</td>
<td>7</td>
<td>5</td>
<td>2</td>
<td>4</td>
</tr>
<tr>
<td>5</td>
<td>5</td>
<td>7</td>
<td>-2</td>
<td>4</td>
</tr>
<tr>
<td>6</td>
<td>9</td>
<td>9</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>7</td>
<td>8</td>
<td>8</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>8</td>
<td>10</td>
<td>10</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>9</td>
<td>2</td>
<td>2</td>
<td>-1</td>
<td>0</td>
</tr>
<tr>
<td>10</td>
<td>4</td>
<td>3</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>$\Sigma d^2 = 13$</td>
<td></td>
<td></td>
<td></td>
<td>8</td>
</tr>
</tbody>
</table>
Group 4 (private ports), Spearman’s Rank Correlation Coefficient

\[
r_{s41} = 1 - \frac{6\sum d^2}{n(n^2-1)} = 1 - \frac{6(14)}{10(99)} = 1 - \frac{84}{990} = 0.915
\]

\[
r_{s42} = 1 - \frac{6\sum d^2}{n(n^2-1)} = 1 - \frac{6(8)}{10(99)} = 1 - \frac{48}{990} = 0.951
\]

Table 3 Rankings of events by survey participants from each group in round 1 to round 2. The correlation of rankings of events for these groups is same, that is 0.951.

<table>
<thead>
<tr>
<th>Event</th>
<th>Round 1 (R1)</th>
<th>Round 2 (R2)</th>
<th>Difference between Rank1 and Rank2</th>
<th>(d^2)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>SP 1 2</td>
<td>SP 1 2</td>
<td>R1 2</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>1 1</td>
<td>1 1</td>
<td>0 0</td>
<td>0 0</td>
</tr>
<tr>
<td>2</td>
<td>2 2</td>
<td>2 2</td>
<td>0 0</td>
<td>0 0</td>
</tr>
<tr>
<td>3</td>
<td>6 4</td>
<td>6 5</td>
<td>2 1</td>
<td>1 1</td>
</tr>
<tr>
<td>4</td>
<td>3 3</td>
<td>3 3</td>
<td>0 0</td>
<td>0 0</td>
</tr>
<tr>
<td>5</td>
<td>5 6</td>
<td>5 6</td>
<td>-1 -1</td>
<td>1 1</td>
</tr>
<tr>
<td>6</td>
<td>9 7</td>
<td>9 8</td>
<td>2 1</td>
<td>1 1</td>
</tr>
<tr>
<td>7</td>
<td>7 9</td>
<td>7 9</td>
<td>-2 -2</td>
<td>4 4</td>
</tr>
<tr>
<td>8</td>
<td>10 10</td>
<td>10 10</td>
<td>0 0</td>
<td>0 0</td>
</tr>
<tr>
<td>9</td>
<td>4 5</td>
<td>4 4</td>
<td>-1 -1</td>
<td>1 1</td>
</tr>
<tr>
<td>10</td>
<td>8 8</td>
<td>8 7</td>
<td>0 0</td>
<td>1 0</td>
</tr>
</tbody>
</table>

\[2d^2 = 14\]

The Spearman’s rank correlation coefficient for group 2 (USCG) participants was 0.56 and 0.80 on survey rounds 1 and 2, respectively. For group 3, (shipping industry) participants the correlation coefficient was 0.922 and 0.951 on survey rounds 1 and 2, respectively. Group 4 (private ports) participants correlation coefficient on survey round 1 was 0.916 and round 2 was 0.951. The agreement between survey participants from group 2 (USCG), group 3 (shipping industry), and group 4 (private ports) improved from survey round 1 to round 2. The correlation of rankings of events between survey participants from group 2; \(r_{s22} = 0.80\), group 3; \(r_{s22} = 0.951\), and group 4; \(r_{s22} = 0.951\) are close to + 1 respectively which indicates that there is a solid positive correlation between survey participants from each group in rankings of events that could disrupt operations on the Sabine – Neches waterway for more than 24 hours.

V. CONCLUSIONS

- Experts in each group tend to agree and perceive these events or scenarios with a common perception and there opinions are homogeneous
- There is better agreement on ranking of events by experts from group 3 (shipping industry) than group 2 (USCG).
- Experts from group 3 (shipping industry) and group 4 (private ports) perceived these events on a common ground since the spearman’s rank correlations coefficient for these groups is same, that is 0.951.
- Analysis of expert judgment can be utilized for drawing conclusions on the agreement between experts on a collective basis.

REFERENCES