Military Operations Research,
Vol. 7, No 4, pp. 5-20 December 2002

Military Operations Research:
Best-Paper Award for 2002

Probabilistic Modeling of Terrorist Threats: A Systems Analysis Approach to Setting Priorities Among Countermeasures

Elisabeth Paté-Cornell
and Seth Guikema
Department of Management Science and Engineering
Stanford University

Abstract
Since the terrorist attacks on the United States on September 11th 2001, a large number of potential attack scenarios have been generated, and a number of responses have been implemented or suggested. The spectrum of possibilities, however, is extremely large, the amount of existing or potentially relevant information immense and confusing. The effectiveness of countermeasures can be difficult to assess in the absence of some quantification of the risks posed by different scenarios. We present in this paper a model for setting priorities among threats and among countermeasures, based on probabilistic risk analysis, decision analysis, and elements of game theory. This model accounts for the probabilities of different scenarios, the objectives of both the terrorists and the U.S., and the dynamic competition between them. In this paper, we use the rational decision analysis model in a descriptive mode on the terrorist side and in a prescriptive mode for the United States. Because we illustrate our model using fictitious numbers, the importance of this work is not so much in the specific ranking of countermeasures that it suggests as in the framework for reasoning that it provides. This includes analysis and fusion of data from many sources and with different levels of reliability to understand the situation, and explicit preferences to set priorities in the face of considerable uncertainty.

KEYWORDS: Threat analysis, Risk Analysis, Probability, Decision Analysis, Countermeasures, Asymmetric Warfare, Game Theory, Homeland Defense

Military Operations Research,
Vol. 7, No 4, pp. 5-20 December 2002

PROBABILISTIC MODELING OF TERRORIST THREATS: A SYSTEMS ANALYSIS APPROACH TO SETTING PRIORITIES AMONG COUNTERMEASURES

1. INTRODUCTION

Since the terrorist attacks on the United States on September 11th 2001, a large number of potential attack scenarios have been generated at variable levels of detail, and a number of responses have been implemented or suggested. The spectrum of possibilities, however, is extremely large, the amount of existing or potentially relevant information immense and confusing, and the effectiveness of various measures difficult to assess in the absence of some quantification of the risks posed by different scenarios. In that context, the problem is to assess the risk reduction benefits of different countermeasures and their costs, both in monetary terms and in terms of civil liberties or mere inconvenience.

We present here a relatively simple global model of the spectrum of terrorist threats based on systems analysis and probability. The objective is to bring some order in the mass of available information and to describe the links between the key elements of the different classes of scenarios. The model can then be used to rank the threats along several dimensions of the consequences of attack scenarios, and to assess the benefits of threat reduction measures. This probabilistic model has a classic risk analysis structure and can be represented as a decision tree, or more conveniently as an influence diagram, at least in its static version (i.e., a snapshot of the situation at any given time).

The probabilistic description of each event and variable of this model can itself be the result either of a much more detailed model or of the encoding of expert opinions. There is thus a definitely subjective aspect to this model: some of the probabilities may be based on frequencies of past events, but most are the opinions of the best available experts. These probabilities are then included in the computation of the chances of a specified scenario. Alternatively, one can interview some of the best policy analysts and ask them to rank directly threats and countermeasures; but the results may reflect classic biases grounded in the nature of the last attack or in a professional familiarity with some terrifying scenarios. Therefore, one advantage of the systems analysis and probabilistic approach is that the different domains of expertise can be represented by the most qualified experts in each particular field such as specific biological threats, existence of loose nuclear material, transportation of explosives, preferences and skills of the perpetrators, etc. This approach therefore limits the eventual effects of biases and errors in the assessment of each variable.

2. OVERVIEW OF THE MODEL STRUCTURE AND OBJECTIVES

Several levels of systems analysis are needed to implement this model to the point where it is detailed enough to support decisions to adopt various countermeasures.

First one needs an *overarching model* to bring together the mass of information regarding different types of threat scenarios, different groups of perpetrators, their objectives and the damage that they can cause. The consequences depend on the effectiveness of their "supply chain" (people and skills, cash, material and communications), as well as that of the U.S. response. One of the components of that model is the choice of a target (or set of targets) by the perpetrators, and an assessment of the effects of an attack on these targets.

Therefore, second, one needs an analysis of the different potential targets, including infrastructure systems and networks (e.g., the water distribution system in Massachusetts) or specific targets (e.g., a U.S. military facility in the Middle East), in order to find the vulnerabilities of each of them. This second level needs to include a representation of the effects of interdependencies among networks and systems that constitute potential targets. These could be, for example, the effects of the loss of electric power on the operations of the communication system, the flooding damage caused by a breach in a dam, or the loss in reconnaissance capability caused by an attack on U.S. reconnaissance assets. One can then identify the most effective reinforcement measures such as redundancies, shielding, or other ways of increasing a system's robustness.

Third, one needs to assess the consequences of the different attack scenarios. To that effect, one has to define the dimensions or attributes of these consequences, one of which is the level of economic losses. These include direct and immediate losses but also the secondary ("ripple") effects of primary damage to different parts of the infrastructure(s) that may imply interruption of economic production, consumption, or threat to the U.S. defense system. These secondary losses could be, for example, the secondary economic effects of network failures e.g., the effects of interruptions of telecommunications on the banking system, or electric distribution on manufacturing.

The focus of the rest of this paper is on the *overarching model* (the first level) with the objective of supporting decisions and setting priorities among homeland defense countermeasures. The model described here is designed to gather diverse kinds of information, and is based on risk analysis (Apostolakis, 1990), decision analysis (Raiffa, 1968; Keeney and Raiffa, 1976), systems analysis and game theory (Gibbons, 1992), including the dynamics and game aspects that are needed to permit updating over time. This pilot model is not a finished product but a blue print for a global, more detailed model that could then be used and updated in real time to support protection decisions. Its ultimate objective is to identify:

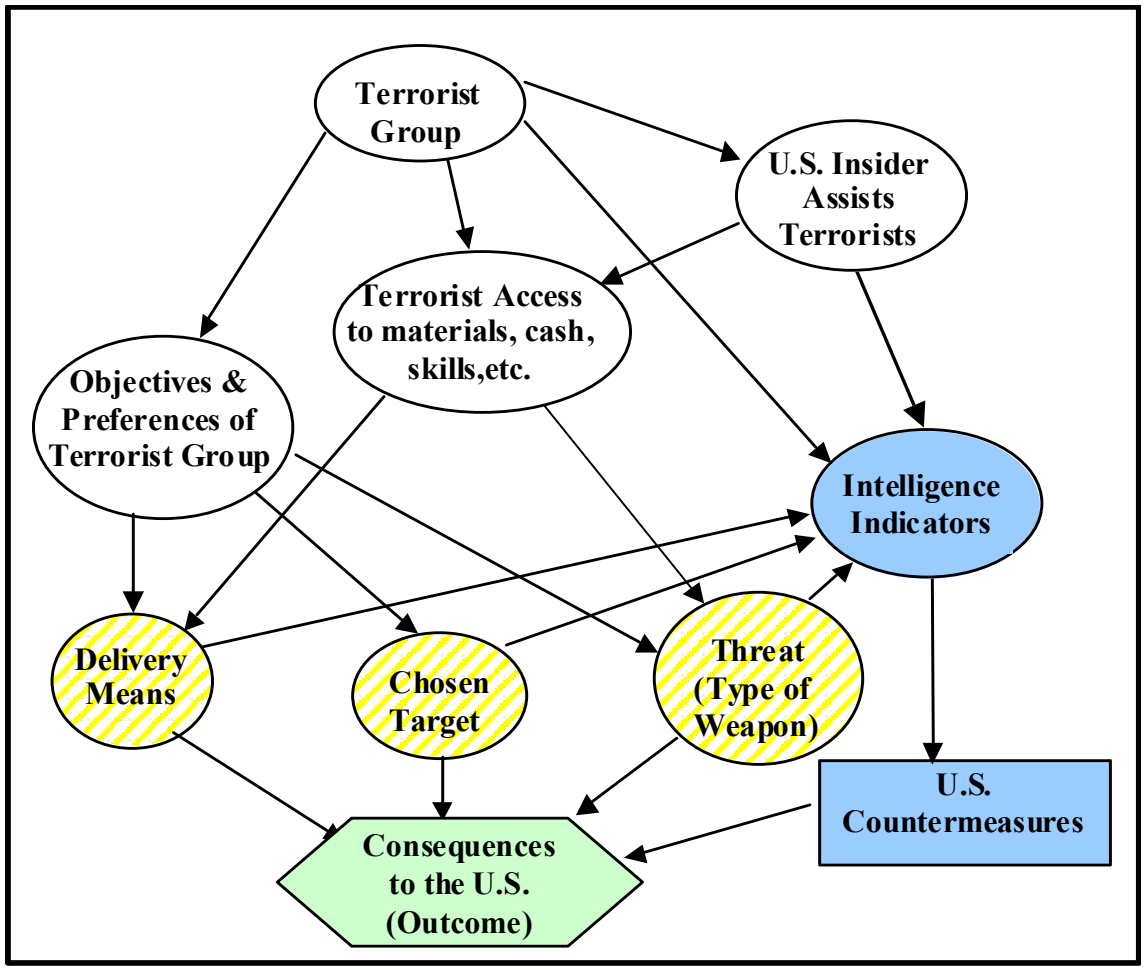
- The elements of the US infrastructure, networks and socio-economic components that need to be strengthened in priority order
- The most effective means of reducing the overall threat, for example, by disruption of the terrorists' supply chain (cash, people and skills, materials and communications, etc.)
- The type of intelligence information that needs to be gathered in priority, focusing on the quality, the timeliness, and the relevance of the signals given resource constraints (costs, people, space assets, etc.).

The plan is thus to use this capability-based, effects-based approach to set priorities among countermeasures, and to target intelligence gathering in order to ensure the effectiveness of the efforts involved on the U.S. side given the costs and the benefits of the different countermeasures.

3. MODELING SCENARIOS OF TERRORIST ATTACKS ON THE U.S. AND U.S. INTERESTS

Our overarching model is based on the engineering risk analysis method (e.g., Modarres et al., 1999; Apostolakis, 1990). It is represented in Figure 1 in the form of an influence diagram, the different nodes of which are discussed further.

.



Legend: Oval nodes: uncertainties about events and random variables. White nodes: uncertainty about terrorist groups and their activities, including (striped) the elements of an attack scenario. Grey nodes: U.S. side. Square node: decision node. Hexagonal node: consequences to the U.S. of an attack scenario given countermeasures. Arrows: probabilistic dependencies

.

Figure 1: Influence diagram representation of an overarching model for the prioritization of threats and countermeasures.

In an influence diagram such as that shown in Figure 1, an oval node represents a random variable or event with its possible realizations, and the probabilities assigned (here, on the U.S. side) to each of these realizations. A rectangular node represents a decision (here, made by the U.S.) and is characterized by the possible options. In Figure 1, we represented each attack scenario by a combination of the realizations of the shaded oval nodes, i.e., the combination of a target (e.g., a public building), a type of weapon (e.g., a conventional explosive) and a means of delivery (e.g., a suicide bomber). The arrows in Figure 1 represent probabilistic dependencies among the events, state variables or decision variables shown in the diagram nodes.

The first step in the analysis is to combine probabilistic modeling of the actions of different groups of terrorists with an assessment of their objectives and of the consequences for U.S. interests. This part of the analysis permits:

- Identification of an exhaustive set of *classes* of attack scenarios.
- Assessment of the likelihood of occurrence of these classes of scenarios based on intent, chances of success given intent, and attractiveness from the point of view of the perpetrators.
- Prioritization of these attack scenarios based both on their likelihood and on the expected damage to the U.S. if they occur (i.e., from the U.S. point of view).
- Modeling of the dynamics of the situation as a "game" between the different parties with learning on both sides, by updating both the model and the parameter values after each time period.

Risk analysis is based on systems analysis and Bayesian probability (Apostolakis, 1990). It is particularly appropriate in this case for several reasons. First, it allows the combination of data about the different aspects of the problem from different sources of information. Therefore, it provides a framework for ranking countermeasures in a situation where one has only limited past experience. Given the scarcity of the experience base regarding terrorist attacks in the present context, the emphasis is on the model's reasoning and structure rather than on the numerical values. The model allows identification of the effects of different factors and parameter values on the conclusions and recommendations and therefore, of the most critical parameters about which additional information may be most valuable.

The key variables of the overarching model are:

- The different groups or individuals who can be potential perpetrators (e.g., Islamic fundamentalist groups),
- The objectives of these groups (and the weight of the different attributes of the objectives in their preferences and tradeoffs),
- The means at their disposal (material, skills, cash, and means of communication),
- The nature of the potential threats (nuclear, biological, conventional, etc.),
- The different classes of targets (e.g., buildings, networks, individuals or groups of individuals), and
- The means of delivery (e.g., ships or airplanes).

The different realizations of these variables (which are described in the appendix) influence the feasibility and effectiveness of intelligence gathering. For example, some foreign groups or some targets are easier to monitor than others. Given specific information, some immediate measures can be taken in some cases, but the data may be much more difficult to use in others. For example, it may have been known at the beginning of September 2001 that some of the terrorists that ultimately perpetrated the 9/11 attack on the U.S. had slipped into the country, but at that time the danger was not clear.

Therefore, in addition to the previous variables that describe the potential terrorist groups, their means and their intentions, the model includes:

- The intelligence information gathered by the U.S. and their allies,
- The subsequent countermeasures, and
- The resulting level of damage given a totally or partially successful attack.

Which groups are most likely to plan an attack, the objectives of these different groups, and the corresponding types of attack are thus key variables of the overarching model. For instance, it seems that the explosion of a nuclear warhead, if feasible at all, may be more attractive to an Islamic fundamentalist group than to disgruntled Americans. The analysts thus need the help of social scientists who are most able to shed some light on issues of objectives including the possible shift in preferences with changes in the availability of means. In turn, the intelligence community may then find this information useful in its decision of how best to use its assets.

In a coarse numerical illustration of the static model described here, we generated the probabilities of each class of scenario as a function of the intents of each group, the feasibility of different types of attack for that specific group given its "supply chain", and the level of attractiveness of a successful attack given the group's objectives based on our own assessment of probabilities and data. One can assume, for instance, that for each particular type of threat, the choice of each of the attack scenarios given intent are independent, and that the probability of a given scenario is proportional to:

- The chances of involvement of the different groups ("intent"),
- The probability of success conditional on intent, based on the effectiveness of the group in carrying out the planning and implementation of the threat scenario given their supply chain, and
- The level of attractiveness of the scenario consequences measured by the value of the preference attributes for the group.

One key assumption of this model is thus the use of the rational decision analysis model in a descriptive mode. The axioms of rationality were proposed originally by von Neumann to describe the behavior of the rational consumer (von Neumann and Morgenstern, 1953). Subsequently, however, they were generally used in the normative mode as it was recognized that in reality, human behaviors generally violate these axioms. For example, people show circularities in preferences, do not account for

probabilities of outcomes (which they often do not know how to evaluate), and do not necessarily satisfy the "sure thing principle" (Savage, 1954). The school of decision analysis that is based on these axioms (or equivalent sets of axioms) leads to the maximization of expected utility of an identified, single decision maker (e.g., Howard, 1966, Raiffa, 1968). The same model, however, can also be used in the normative mode to describe situations in which a group generally acts in a coherent fashion, within a set of constraints, accounting for the probabilities of success of its operations, and with a generally consistent set of objectives. From the point of view of the U.S. analysts trying to anticipate these behaviors, this approach requires estimating the potential perpetrators' utilities of the possible outcomes of different types of attacks, and their expectations about their chances of success. This implies a sense of what the perpetrators are trying to achieve, and of what they know of the effects of their actions, and about the countermeasures that may have been implemented. An alternative here would be to use prospect theory (Khaneman and Tverski, 1979), which would require a more complex set of descriptive data, for example, about the preferences of the perpetrators for operations outcomes, both in the positive and the negative domains.

The data used in the model thus represent the beliefs of U.S. experts regarding the probabilities of actions and the value systems of the different groups of perpetrators because the model is designed to support U.S. decisions and is based on U.S. knowledge. It should thus be noted that in the dynamic/game-theoretic stage described further, each side puts a probability distribution on the beliefs of the other.

In a simple first illustration we use the following notation.

- S: Successful attack (of any kind)
- j: index of terrorist group G_j (e.g., Islamic fundamentalists)
- i: index of weapon chosen (type of threat, e.g., a biological attack) for an attack attempt
- k: index of the different attributes of the preference (utility) function of the terrorist groups
- $v(X_{ijk})$: Value of attribute k (e.g., the number of casualties inflicted) for terrorist group j (e.g., Islamic fundamentalists) in the case of a successful attack with weapon i (e.g., a biological attack).
- U_j: Utility function (preferences) of group j
- W_i: Choice of weapon (e.g., a biological attack) for an attack attempt
- I_j: Intent from group j to attack in the next time period (including all types of threat)
- P_{US}: probability as assessed by the US to represent the US beliefs
- P_{TE}: probability as assessed by the US of a terrorist probability estimation (e.g., of their own chances of success in a specified attack scenario)
- $E_{US}(.)$: expected value of a random variable as assessed by the US for themsleves
- E_{TE} (.): US assessment of the expected value of a random variable as viewed by the terrorists

- $v(Y_{ik})$: Value of attribute k (e.g., casualties inflicted) for the U.S. in the case of a successful attack with weapon i (e.g., a biological attack).
- $\underline{U}_{US}(S, W_i)$: disutility to the US of a successful attack of type i along the different attributes Y_k

In our simple first illustration we assume that the U.S. experts estimate the probability of each attack scenario according to the following steps.

1. U.S. analysts assess the expected utility of each attack scenario for each possible group of perpetrators based on their own (U.S.) beliefs about terrorists' beliefs and preferences. This step requires incorporation of the U.S. assessment of the terrorists' beliefs about their chance of success if they launch the different types of attack and of the terrorists' utility functions. The result of this step is an assessment, by the US, of the expected utility to the terrorist group j of an attack using weapon i (Equation (1)).

$$E_{TE}\left(U_j \mid W_i, I_j\right) = P_{TE}\left(S \mid W_i, I_j\right) \times U_j\left(S \mid W_i, I_j\right) \tag{1}$$

   In equation (1), the utility to the terrorist group j of a successful attack of type i is assumed to be simply the sum of the attributes of scenario i for group j as shown in equation (2). However, many other forms of utility functions such as multiplicative and multi-linear are possible (Keeny and Raiffa, 1976). The assumption that a simple sum is an appropriate utility function must be carefully checked in practice.

$$U_j\left(S \mid W_i, I_j\right) = \sum_k v\left(X_{ijk}\right) \tag{2}$$

2. The expected utilities of the different possible attack scenarios for each of the different groups as computed in step one are renormalized to provide probabilities of terrorists actions W_i for each group conditional on that group intent I_j to launch an attack. This approach implies that the probability that an attack W_i of a specific type is launched in a particular time period is directly proportional to the expected value of the attack scenario to the terrorists relative to all other attack possibilities that they could consider. In other terms, the probability of a specific attack scenario is a function of the perception, by each group, of their probability of success and of their preferences regarding the possible outcomes of that scenario. If the U.S. knew the terrorists' utility functions with certainty, we could model each group's choice as the highest expected-utility option with probability one. To some degree, our approach thus reflects the U.S. uncertainty about the terrorists' utility functions. The computation of the probability of each type of scenario W_i, given intent to attack by group j (I_j) as assessed by the US for each group is given in Equation (3). It assumes that at every time period, each terrorist group plans only one type of attack, and that the probability of a specified type of attack is proportional to the ease of execution and the damage inflicted on the U.S. The assumption that each group can plan one and only one type of attack is a

simplifying assumption. If this is not the case, then Equation (3) would need to be modified to compute joint probabilities of various combinations of types of attacks.

$$P_{US}(W_i \mid I_j) = \frac{E_{TE}(U_j \mid W_i, I_j)}{\sum_i E_{TE}(U_j \mid W_i, I_j)} \tag{3}$$

As discussed earlier, Equation 3 assumes that the potential perpetrators behave as rational decision makers, i.e., that they choose in priority what is more likely to succeed and to achieve the higher level of utility on their part. Equation 3 also assumes that the different attack scenarios are collectively exhaustive and mutually exclusive (their probabilities add up to 1), i.e., that at a given time a group focuses in priority on one type of attack.

3. Each terrorist group knows with certainty whether they are actually planning an attack in the next time period (there is no uncertainty from their perspective about I_j). From the US point of view, the intent of each group is uncertain. That uncertainty needs to be represented by a prior probability of attack, based for example, on intelligence information or on past experience with the average frequency of attacks by that group. To compute the probability from the US point of view of an attack of a specified type in the next time period, the probabilities found in the second step (Eq. 3) are multiplied by a base rate (prior probability) of an attack of any kind by each group j in the next time period as estimated by the U.S. (Equation (4)).

$$P_{US}(W_i, I_j) = \frac{P_{US}(I_j) E_{TE}(U_j \mid W_i, I_j)}{\sum_i E_{TE}(U_j \mid W_i, I_j)} \tag{4}$$

The probability of success S of an attack of type i by group I_j is then the product of the probability of attack attempt of type i (W_i) by group j multiplied by the probability of success given an attack of type i by group j (some group maybe better than others at implementing specified attack types) :

$$P_{US}(S, W_i, I_j) = P_{US}(S \mid W_i, I_j) \times P_{US}(W_i, I_j) \tag{5}$$

The total expected number of successful attacks of type i [$EN_{US}(S,W_i)$] is the sum of the probabilities of such successful attacks for all potential terrorist groups that intend to carry them out. If the probabilities of successful attacks by the different groups are very low, then this is approximately equal to the probability of a successful attack of each type.

$$EN_{US}(S,W_i) = \sum_j P_{US}(S,W_i,I_j) \tag{6}$$

4. The disutility (negative impact) to the U.S. of a successful attack scenario i, is assessed, and this assessment is combined with the expected number of successful attack attempts (successful in the sense of being attempted) of different types found in step 3 and with the U.S. assessment of the likelihood of success of each type of attack if it were to be launched to compute the expected disutility of such an attack to the U.S. in the absence of additional intelligence information and countermeasures beyond the *status quo*.

$$E\underline{U}_{US}(S,W_i) = EN_{US}(S,W_i) \times \underline{U}_{US}(S,W_i) \tag{7}$$

$$\underline{U}_{US}(S,W_i) = \sum_k v(Y_{ik}) \tag{8}$$

In equation (7), the expected disutility to the US of a successful attack S_i is the sum of the negative values attached to each of the attributes $v(Y_k)$ in case of S_i. In other terms, in equation (8) as in equation (2), we assume "additive independence" of the utility or disutility functions.

5. The changes of the probabilities of success of the different attack scenarios i for each of the considered groups j for each possible countermeasure and level of intelligence information are then assessed in order to examine the benefits of the different countermeasures. These countermeasures can affect either the probability of an attack (e.g., by decreasing the perceived or real probability of success from the terrorists' view point) or the consequences of an attack, therefore the disutility of the consequences to the US. The countermeasures that yield the largest decrease in disutility to the U.S are then identified based both on costs and benefits.

4. A SIMPLE ILLUSTRATION OF THE PRINCIPLES

We present first an illustration of the general way in which the probability and consequences of an attack are computed. We then show how to compute the benefits of various countermeasures in a more elaborate model in which the realizations of each random variable and event are more complex.

Assume for example, that we consider only two groups of perpetrators, Islamic fundamentalists (IF) and American disgruntled (AD) and four potential threats: a nuclear warhead explosion, a nuclear incident (i.e., a "dirty bomb"), a smallpox attack, and a repeated attacks with conventional weapons on urban areas ("conventional attacks"). Table 1 shows hypothetical data that can be used in the computation of the attractiveness of a successful attack to each group. The value function of the different groups is characterized, for simplicity, by three attributes (X_k), the symbolism of the attack (X_1),

the amount of destruction the attack causes (X_2), and the degree to which the attack leads to political destabilization (X_3). We assessed what we believe to be (from the U.S. point of view) the values to the perpetrators (group j) of each type of weapon attack (i) along the lines of these three attributes (k). We quantify these value assessments on a scale from 1 to 10 (intended in this simple example to be representations of single-attribute utility) and we weight them equally in an additive-independent measure of the perpetrators' utilities U_{ij}.. In practice, sensitivity analysis would be needed to examine to different weightings of the attributes. This assumption of additive independence is later relaxed. Table 1 shows the value of these attributes for each group and each type of weapon, and the corresponding terrorists' expected utilities.

Table 1: Illustrative data and terrorist utility calculation for the basic model

Nature of the threat (weapon)	**Group**	**P_{TE}(Success| Intent [I_j] and weapon [W_i])**	**Attractiveness to perpetrators of successful outcome of W_i**				**Expected utility to the terrorist groups**
			X_1	**X_2**	**X_3**	**Total Utility U_{ij}**	
Nuclear warhead explosion	IF	0.01	10	10	10	30	0.27
	AD	-	-	-	-	-	-
Nuclear incident	IF	0.5	8	3	5	16	5.6
	AD	0.5	4	2	5	11	1.1
Smallpox attack	IF	0.7	2	7	8	17	8.3
	AD	0.6	2	7	8	17	3.1
Continuous conventional attack on urban areas	IF	0.9	4	2	9	15	12.2
	AD	0.9	4	2	9	15	12.2

Legend: X_1 symbolism of the attack, X_2 number of casualties and amount of destruction the caused by the attack, and X_3 degree to which the attack leads to political destabilization and erosion of U.S. power.

In this illustrative example, the probability of a successful attack on the U.S. and the expected disutility (negative value) for the U.S. can be computed as shown in Table 2. We have assumed that per time period, there is a 40% chance that the Islamic Fundamentalist group attempts an attack across the spectrum of possible weapons ($p(I_1)$ = 0.4) and a 10% chance that the American Disgruntled group launches an attack ($p(I_2$)= 0.1).

Table 2: Illustrative results for the basic model

Probability of intention: $P_{US}(I_1)=0.4$; $P_{US}(I_2)=0.2$; 1:Islamic Fundamentalists. 2:American Disgruntled

Nature of the threat (weapon) W_i	**Group IF: Islamic Fund. Amer. Disgr.**	**Probability of Attack of type i from group j: $P_{TE}(W_i\|I_j)$**	**Probability of success of attack of type i from group j: $P_{US}(S\|W_i,I_j)$**	**Negative value (disutility) of outcome to the U.S. of a successful attack of type i $\underline{U}_{US}(S,W_i)$**	**Expected disutility of a successful attack of type i to the U.S. $E\underline{U}_{US}(S,W_i)$**
Nuclear warhead explosion	IF AD	0.01 -	0.50 -	-10,000	-20
Nuclear incident	IF AD	0.21 0.07	0.20 0.15	-10	-0.18
Smallpox attack	IF AD	0.31 0.19	0.60 0.60	-100	-8.6
Attack on urban areas with conventional weapons	IF AD	0.47 0.74	0.90 0.50	-10	-2.1

One can then rank the threats (weapons) in several ways; for example, according to the their negative impact on the U.S. given a successful attack (most dangerous course of action); according to their probability of a successful attack (most likely course of action); or according to the negative *expected value* (disutility) of outcome to the U.S. of a successful attack of type i. The importance of the last criterion is to permit setting priorities among countermeasures based both on the probability and the effect of a successful attack of a given type.

Ranking the threats according to "the enemy's most dangerous course of action" does not require the use of probability; it reflects directly the values entered in column 5 of Table 2 and experts' assessment of the potential damage: 1. nuclear warhead explosion; 2. small pox attack; 3. nuclear incident or repeated attacks on urban areas with conventional weapons.

Ranking the threats according to the likelihood of the different scenarios ("the enemy's most likely course of action") is provided by the probabilities of each scenario as shown in column 3 of Table 2. It reflects the enemy's objective but only indirectly the disutility to the US: 1. repeated attacks on urban areas with conventional weapons; 2. small pox attack; 3. nuclear incident; 4. nuclear warhead explosion.

Ranking the threats based on the expected disutilities to the U.S. of the potential losses is provided by the last column of Table 2. 1. nuclear warhead explosion (very unlikely but extremely destructive); 2. small pox attack (much more likely because it is easy to achieve, and quite destructive); 3. repeated conventional urban attacks (very easy to achieve and very damaging in the long run), and 4. nuclear incidents (not as easy to achieve and has relatively limited effects).

Note that these different orders were not necessarily those that came intuitively to the mind of some of the experts who were interviewed to shape the model. For example, some of them tended to underestimate the potential negative aspects of repeated

conventional urban attacks; or to overestimate the destructive potential of a nuclear incident (compared to a nuclear warhead explosion); also, some of the experts of bio-terrorism tended to focus more on the biological threats than the nuclear weapons experts did. Although one could thus question the validity of using the decision analysis model in the descriptive mode, these authors believe that these discrepancies were generally the results of "availability" and "retrievability" biases (Tversky and Kahneman, 1974, Slovic et al., 1979): what came to mind first was not the result of an exhaustive search but rather on immediate recalls of the most recent incidents or discussions. In fact, some of the experts who were interviewed were often willing to admit that they had not truly attempted to include explicitly in their comparisons the likelihood of scenarios with which they were less personally familiar.

5. A SINGLE-PERIOD, TWO-SIDE GLOBAL INFLUENCE DIAGRAM

The same principles are now applied to a more complete (but still very schematic) representation of the problem in which both sides act in response to their beliefs about the intentions and capabilities of the other side. Figure 2 represents an influence diagram that was used in the illustration of this quantitative systems analysis at a global level for a single time period. The left side of Figure 2 represents an influence diagram from the perspective of the terrorists (e.g., the terrorists make the decisions about targets, means of delivery, and nature of the threat), and the right side of the figure represents an influence diagram from the perspective of the U.S. These two diagrams are separated to keep the decisions made by the two different groups separate. This aids in interpreting the diagram, and it is necessary for many of the software packages used to evaluate influence diagrams. In these influence diagrams, the utility of outcomes to terrorist groups is assumed to depend only on the symbolism of the attack and on the loss of life, and the utility of outcomes to the U.S. is assumed to depend only on the symbolism of the attack, the loss of life, and the direct economic consequences of countermeasures. Clearly many other attributes would be of interest in a real implementation of this model (e.g., political destabilization, direct and indirect economic losses, loss of military assets, etc.). The model presented in Figure 2 is meant to demonstrate the method in a more realistic, yet still very schematic, way.

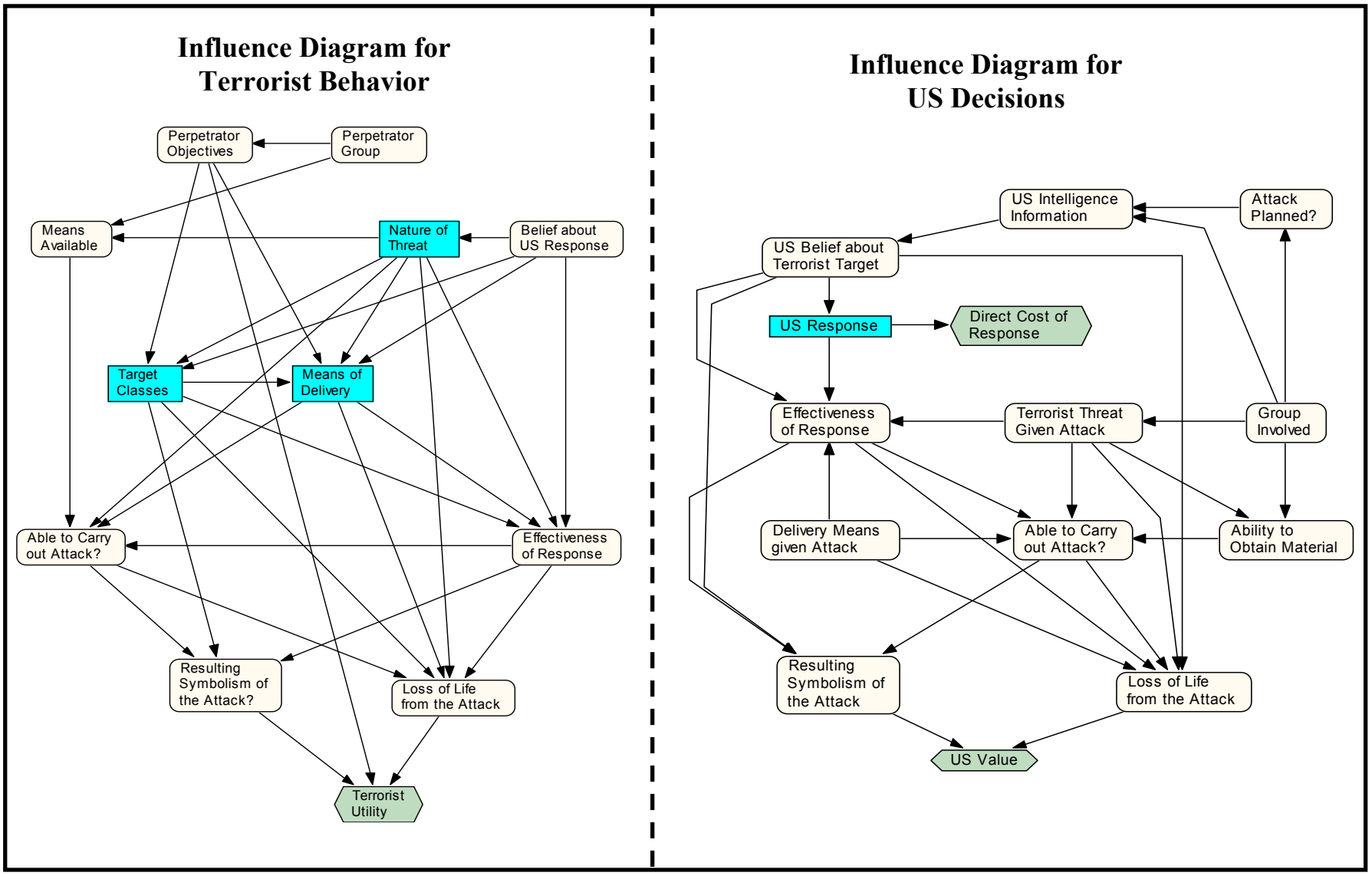


Figure 2. Single-period influence diagrams for the terrorists' and U.S. decisions.

5.1 Use of the Single-period Two-side Model to Assess the Effects of Countermeasures

To use the model presented in Figure 2, the U.S. analysts input their assessments of the terrorists' beliefs in the left side of the diagram, including the utility functions of the different terrorist groups (possibly assigning probabilities to the different possible utility functions). Based on these assessments, the U.S. then computes the expected utility of the different scenarios to the different terrorist groups. As shown earlier, these expected utilities are renormalized as probabilities and then multiplied by the assessed likelihood that each of the groups attempt an attack (the base rate). This information is then used to assess the probabilities of the different attack scenarios by the different groups in the U.S. influence diagram, on the right side of the Figure 2. The U.S. assessments of the likelihood of attacks on different targets, of the different delivery means, and of the different types of weapons are therefore based on the U.S. beliefs about the terrorists' utility functions, beliefs, and abilities. A key factor of the successful implementation of an attack given intent is the effectiveness of the terrorists' "supply chain", including people and skills, cash, materials and communication links. Therefore, US intelligence about these is essential to this kind of knowledge.

In this two-side influence diagram (Figure 2), we consider five possible types of perpetrators: Islamic fundamentalist groups or individuals, disgruntled American groups or individuals (e.g., anti-government, anti-technology, etc.) and foreigners with anti-U.S. dispositions (anti-globalization, anti-U.S. military action, etc.). These groups encompass those that are currently perceived as potential threats, but others can be added.

A key element of the U.S. response is the "disutility" that represents the (negative) preferences of the U.S. In this expanded model, our measure of the disutility of a successful attack incorporates three attributes: the direct economic cost of countermeasures (D), the symbolism (and for the U.S. the loss of prestige and influence), (Sy), and the number of lives lost (L). The symbolism of the attack is measured by an indicator variable that varies from 0 to 1 as follows: 0 for an attack outcome that has little symbolic effect on the U.S. (e.g., an attack that causes moderate damage to a suburb of a middle-size city); 0.5 for an attack scenario with mixed symbolic value (e.g., an attack that partially destroys the headquarters of a large software company), and 1 for an attack scenario with obvious symbolic value (e.g., an attack that destroys the Statue of Liberty).

Clearly, the values of the three attributes of the disutility function depend on the type of attack W_i and the attributes values for each type of attack is indexed in i. The multiplicative factors included for illustration in this function imply that if the monetary unit is one million dollars, the number of live lost is multiplied by 10 million and the scale Sy has been designed to reflect 3 million dollars per unit. These factors have been chosen here arbitrarily and could be changed to reflect other preferences. Furthermore, we have assumed here linearity of preferences. A concave (e.g., exponential) function could be used instead to reflect other risk attitudes, and non-additive utility functions could also be used. With the assumptions given above, the expected disutility to the U.S. is given by Equation (9).

$$E\underline{U} = \sum_i p_i(S, W_i) x [10L_i + 3Sy_i + D_i] \quad (9)$$

5.2 Illustration of the Single-period Two-side Model: Ranking of threats

The illustrative results obtained through the single-period, two-side influence diagram of Figure 2 are slightly different from those obtained through the simple, single-period model presented earlier. When combining the US assessments of the probabilities of success of the different scenarios and of the capabilities and preferences of various terrorist groups, the output of the left side of Figure 2 are the results shown in Table 3.

Table 3. Illustrative results for the marginal probabilities of classes of attack scenarios without countermeasures (*status quo*). **Note: these figures are based on fictitious numbers and do not attempt in any way to represent actual beliefs.**

Class of Scenarios	Approximate Probability of Occurrence per time unit
All scenarios involving attack with a nuclear warhead	7.8×10^{-4}
All scenarios involving attack with a biological weapon	9.8×10^{-4}
All scenarios involving attack with conventional explosives	1.9×10^{-3}
All scenarios involving an attack on a government building	1.2×10^{-3}
All scenarios involving an attack on an urban population	6.8×10^{-4}
All scenarios involving an attack on a symbolic building	1.4×10^{-3}
All scenarios involving an attack on a transportation network	4.8×10^{-4}
All attacks made by truck	1.3×10^{-3}
All attacks made by plane	1.0×10^{-3}
All attacks made by individual carriers	1.4×10^{-3}

Table 4: Illustrative results for the expected disutilities of the different classes of scenarios given that each of them is attempted without additional countermeasures (status quo). **Note: these figures are based on fictitious numbers and do not attempt in any way to represent actual beliefs.**

Class of Scenarios	Approximate Expected Disutility to the U.S.
All scenarios involving attack with a nuclear warhead	1.62×10^{5}
All scenarios involving attack with a biological weapon	2.4×10^{3}
All scenarios involving attack with conventional explosives	1.4×10^{3}
All scenarios involving an attack on a government building	3.7×10^{4}
All scenarios involving an attack on an urban population	3.4×10^{4}
All scenarios involving an attack on a symbolic building	3.6×10^{4}
All scenarios involving an attack on a transportation network	3.3×10^{4}
All attacks made by truck	3.0×10^{4}
All attacks made by plane	3.0×10^{4}
All attacks made by individual carriers	3.4×10^{4}

The illustrative results shown in Table 3 indicate that in this hypothetical situation the ranking of types of weapons based on probability per time unit would be:

- Attack with conventional explosives.
- Attack with biological weapons.
- Attack with nuclear weapons.

If however, one considers both the probability and the consequences of each threat combined in an expected disutility function (Table 4), this hypothetical ranking would become:

- Attack with a nuclear weapon.
- Attack with a biological weapon.
- Attack with conventional explosives.

In the short term and for immediate reaction, the former is very useful information. In the longer term, the latter is very relevant to addressing unlikely but extremely destructive attacks that require a sustained effort of research and implementation of countermeasures.

5.3 Implications of the single-period, two-side model for the ranking of countermeasures

The model can then be used to assess, by differences, the net benefits of different countermeasures as the variation of the expected disutility function with and without these measures accounting for their costs.

The first task is to assess the expected disutility with the countermeasures. To that effect, one must add to the direct economic loss in an attack the on-going costs of countermeasures (CT). We therefore assume that *per time period* (here, for instance, one week), the cost (for example) of protecting government buildings is $20 million, urban population centers $300 million, symbolic buildings (other than government buildings) $75 million, and transportation networks $75 million. If applicable, one needs to introduce here the equivalent uniform cost per time unit of a one-time expenditure. Again, these are illustrative numbers and are not meant to represent realistic estimates of actual costs. The benefits of the different counter-measures can then be computed as the reduction either of the likelihood of success for the different types of attack and for each countermeasure, and/or by the variation of the expected disutility function with and without the different countermeasures.

Given these assumptions and for each possible countermeasure indexed in n (CT_n), we thus use a modified version of the US disutility function of equation (9), $\underline{U}_{US}(L_n,S_n,D_n,CT_n)$. As shown in equation 10, the expected value of that disutility per time unit reflects the way in which the countermeasure affects the probability and consequences of a successful attack of type i. These effects are reflected in the dependence of the loss levels on both the type of attack i and the countermeasures n.

$$E\underline{U}_{US}(L_n, Sy_n D_n CT_n) = \sum_i p_i(S_i, W_i \mid CT_n) x[10xL_i(CT_n) + 3xSy_i(CT_n) + D_i(CT_n)] + Cost(CT_n) \quad (10)$$

The data used to illustrate the model are shown in Figures A1 and A2 in the appendix. These two figures represent not only the influence diagrams but also the realizations of the random variables and events and their marginal or conditional probabilities.

The joint probabilities of scenarios used here for illustration are described in the appendix and used as input to the U.S. decision model. The resulting expected disutilities for the U.S. of the four potential countermeasures considered are shown in Table 4. We assume here for simplicity that the U.S. implements one and only one countermeasure per time period, but this assumption can be easily relaxed in further analysis. The effectiveness of each of the potential countermeasures is included in the form of reduced probabilities of the different attack scenarios. For example, protecting government buildings reduces the chance that a terrorist group is able to successfully attack a government building with conventional explosives, nuclear weapons, biological weapons, etc., but it does not affect the chances of successful attacks on urban populations, transportation networks, or non-government symbolic buildings (e.g., the Sears Tower). The analysis shows that different countermeasures are more effective than others at reducing either (or both) the probability of different types of attacks and the expected disutilities of these attacks because certain types of attacks and targets are more likely to be attempted by terrorists. Countermeasures that address these types of attacks and targets are seen to lead to a larger reduction in attack probability and/or disutility.

Table 5. Illustrative Computation of the Expected Disutilities Corresponding to Examples of U.S. Countermeasures. **Note: these figures are based on fictitious numbers and do not attempt, in any way, to represent actual beliefs.**

Countermeasure	**Expected Disutility to the U.S. with the considered measure**
Protect Government Buildings	-9,031
Protect Urban Populations	-18,918
Protect Symbolic Buildings	-9,045
Protect Transportation Networks	-9,367
No Countermeasures	-31,312

Table 6: Illustrative computation of the net benefits of examples of U.S. countermeasures in terms of variation of the probability of a successful attack of each type, given that such an attack is attempted per time unit. **Note: these figures are based on fictitious numbers and do not attempt, in any way, to represent actual beliefs.**

Class of Scenarios	**Conditional Probability of Success per time unit if protecting:**				
	Nothing	**Government Buildings**	**Urban Populations**	**Symbolic Buildings**	**Transpor-tation Networks**
All scenarios involving attack with a nuclear warhead	0.175	0.135	0.164	0.135	0.138
All scenarios involving attack with a biological Weapon	0.180	0.129	0.158	0.121	0.132
All scenarios involving attack with conventional Explosives	0.757	0.523	0.660	0.527	0.536

Table 6 shows, for example, that if the objective were to minimize the probability of a successful attack with conventional explosives given that one is attempted, the ranking of the countermeasures, based on the fictitious numbers that we used for illustration, would be:

- Protect government buildings.
- Protect symbolic buildings.
- Protect transportation networks.
- Protect urban population centers.

Table 7: Illustrative computation of the net benefits of examples of U.S. countermeasures in terms of variation of expected disutilities per time unit **Note: these figures are based on fictitious numbers and do not attempt, in any way, to represent actual beliefs.**

Countermeasure	**Decrease in Expected Disutility (Benefits) Relative to not Implementing any Countermeasure (*status quo*)**
Protect Government Buildings	22,282
Protect Urban Population Centers	12,394
Protect Symbolic Buildings	22,265
Protect Transportation Networks	21,945

Table 7 shows that based on the fictitious numbers that we used for illustration, the ranking of the countermeasures in order of decreasing benefits i.e., their decrease in expected disutility for the U.S,. is:

- Protect government buildings.
- Protect symbolic buildings.
- Protect transportation networks
- Protect urban population centers.

Note that in practice, this last ranking is the most relevant for policy making because it includes the costs of the countermeasures and the probabilities and consequences of the different scenarios with and without them. The ranking of threats, however, may be important in terms of immediate warnings and protection. In all cases, an important feature of this analysis is that it provides a way to identify the factors of the problem that are most affected by various countermeasures.

6. DYNAMICS AND GAME-THEORETICAL ASPECTS OF THE MODEL

The illustration of the model so far focused only on one-time period. In reality, this model needs to be updated at every time period. Each side (i.e., the terrorists and the U.S.) observes the actions of the other side and modifies its probabilistic beliefs about the resources, intents and actions of their opponent in the next time period based on what they have learned during the previous one. The model thus has to be used in a dynamic and game-analytic mode.

The focus of this section is on the *structure* of the game-theoretic model for the dynamic counter-terrorism problem. We do not illustrate it by a numerical application, but its implementation would be similar to that of the single-period model, with the additional step of periodic updating of the model and its input. All realizations and probability distributions of the different events and random variables (U.S. beliefs) must be regularly updated on the basis of the events and new information, if available, based on the signals observed in the previous time period (e.g., intelligence information or foiled attack attempts). More generally, the changes that need to be modeled include moves and countermoves of both sides (U.S. and perpetrators), changes in strategy and means, and lessons learned about the effectiveness of different tactics and strategies. For instance, the model must be updated to include new information about the location of the source of potentially harmful material. Such information in turn, should allow monitoring both the material itself (nature, location, amount) and the people who may have access to it. The model can then be used to compute the benefits of countermeasures designed to avoid dissemination of the material.

Another type of change that needs to be included is the evolution of the organizations involved, the emergence of new groups, or a new structure of existing groups and networks. The al Qaeda network, for instance, has been fragmented by the U.S. attacks in Afghanistan but is likely to reconfigure its operations in a different mode, e.g., on the basis of quasi-independent sub-networks or cells. The different factions are described in the "groups" node, each with different means and "supply chain". A critical aspect of the dynamics involves the political changes, shifts of alliances, and shifts in the policies of existing states and nations. The situation of alliances in the Middle East and Central

Asia is extremely volatile and affects - among other factors - the supply chain of different parts of the terrorist operations. The corresponding changes in the model must be made in the description of the node "groups" and in the nodes that represent the terrorists' supply chain. Another aspect of critical change over time is technological. These changes could include, for example, a breakthrough on the perpetrators' side in the use of existing nuclear weapons, or the development by the U.S. of a biological test that would allow quick detection of small pox at an early stage.

In practice, the analytical maintenance of the model at every time period must thus include updating of:

- The model structure (new factors that translate into new nodes and new links),
- The possible realizations of each variable,
- The probabilities of the different realizations,
- The objective functions of the perpetrators.

Figure 3 shows the structure of a game-theoretic formulation of the overarching model. It focuses on the case in which both sides respond to intelligence information about the other side's actions during the last time period. The line dividing the graph represents the division of "information sets", meaning that the U.S. experts are uncertain about the terrorists' actions and state of knowledge when the U.S. authorities make a decision in the considered time period, and vice-versa. At each time period, both the U.S. and the terrorists make decisions regarding their actions in the upcoming time period based on the information accumulated so far. The probabilities as assessed by each side are noted as p_i for the perpetrators' assessments and q_i for the U.S. As in the earlier illustration and because the model is run by U.S. experts, the p_i's represent the best knowledge that the US experts can gather about the terrorists' beliefs.

7. CONCLUSIONS

In designing and implementing strategies of response to potential terrorist attacks, it is essential to think beyond the re-occurrence of the last event. A systematic analysis permits combination of the relevant events and factors, and, therefore, identification and analysis of a large spectrum of possible scenarios. The model presented here involves, in particular, probabilistic dependencies, and it uses a forward-looking approach to generate a set of possibilities and scenarios. The quantitative approach permits two things that qualitative methods don't: comparison of the net effects of different threats (both in terms of probabilities and consequences) and combination of dependent factors. Therefore, it may help reduce excessive spending on the prevention of what has already happened without eliminating the possibility of improving defense against past types of attacks because it places these previous events in the perspective of a global set of possible scenarios.

In any case, in its practical application, the analysis must include the dynamics of the events and the moves and countermoves of both sides (the U.S. and the perpetrators). The numerical data needed in the implementation of the model will generally come from

several sources: output of another level of systems' analysis (e.g., the vulnerabilities of a communication network), statistics from past observations, or the opinions of experts (including intelligence information) about the different aspects of the problem. Therefore, this approach has the advantage of exploiting the benefits of expertise in different fields, as opposed to the global expertise of policy makers who might generate intuitive rankings of scenarios based on their past experience. Comparison of the results obtained both ways may provide a "reality check" after identification of the potential sources of disagreement. The experts may be shortsighted, but on the other hand, the model may miss something that they intuitively know. A rational systematic approach can thus support better decisions by improving the reasoning of the policy makers while allowing them to inject their intuition in an analysis that may need to be improved to represent the full spectrum of their knowledge.

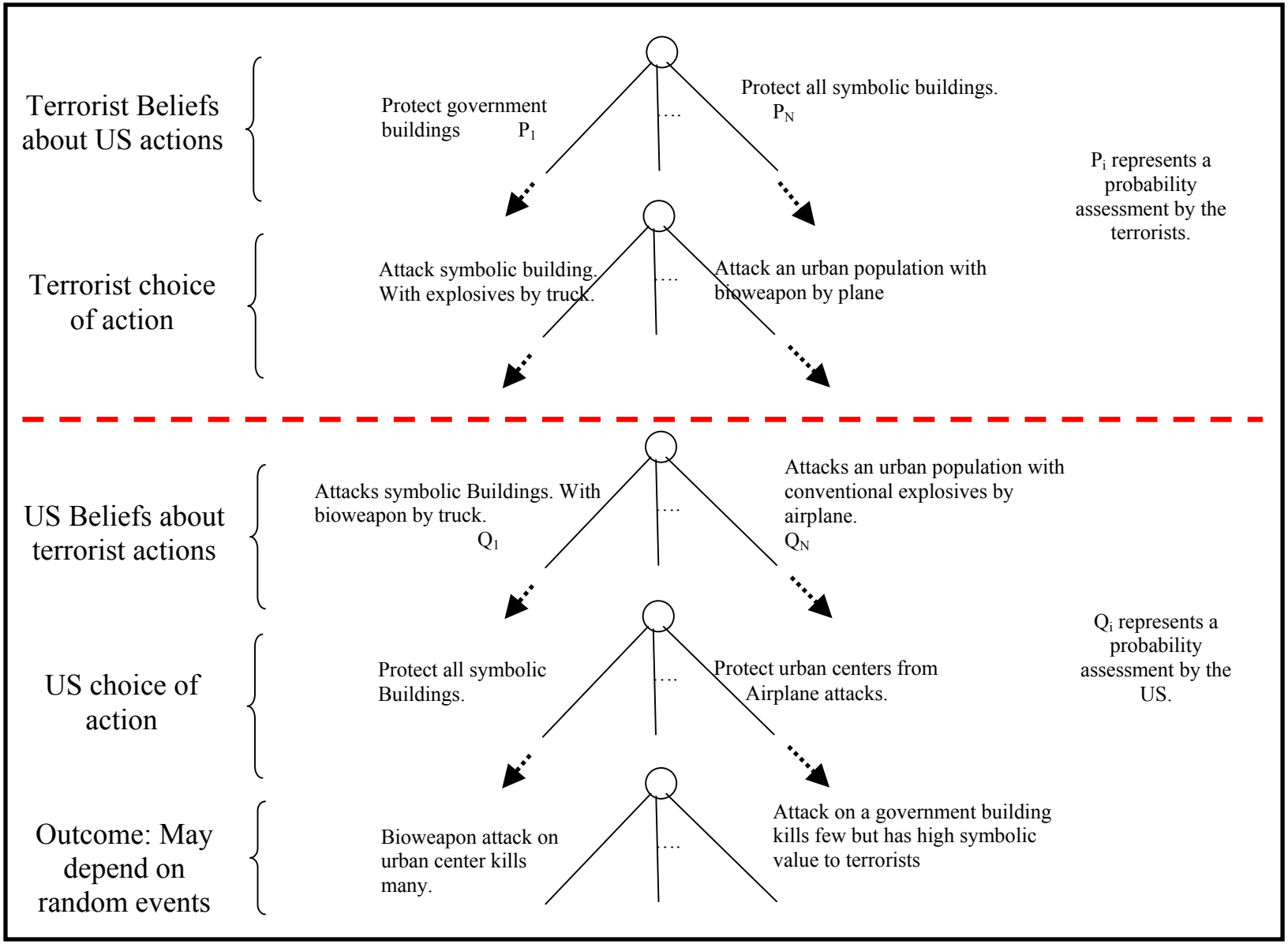


Figure 3. General Game Theoretic Model for the Terrorism Problem.

8. ACKNOWLEDGMENT

This work was supported in part by an NSF grant SES-0079872 and by a National Defense Science and Engineering Fellowship from the Department of Defense.

9. REFERENCES

Apostolakis, G. 1990. The Concept of Probability in Safety Assessments of Technological Systems, Science, Vol. 250, 7 December, 1990.

Gibbons, R. 1992. Game Theory for Applied Economists, Princeton University Press, Princeton, New Jersey.

Howard, R.A., 1966. Decision Analysis: Applied Decision Theory, Proceedings of the Fourth International Conference on Operational Research, Wiley, New York, pp. 55-71.

Howard, R.A. 1990. From Influence to Relevance and Knowledge, *in* Influence Diagrams, Belief Nets, and Decision Analysis, Ed. R.M. Oliver, and J.Q. Smith, John Wiley and Sons, New York.

Khaneman D. and A. Tversky. 1979. Prospect Theory: Analysis of Decision Under Risk, Econometrica, Vol. 47, No. 2, pp. 263-291.

Keeney, R.L. and H. Raiffa. 1976. Decision Analysis with Multiple Objectives: Preferences and Value Trade-Offs. John Wiley and Sons, New York.

Modarres, M., M. Kaminskiy, and V. Krivtsov, 1999. Reliability Engineering and Risk Analysis: A Practical Guide, Marcel Dekker, New York.

Paté-Cornell, M.E.1986. Warning Systems in Risk Management, Risk Analysis, Vol., 5, No. 2, pp. 222-234.

Paté-Cornell, M.E. 2002. Fusion of Intelligence Information: A Bayesian Approach. Risk Analysis, Vol. 22, No. 3, pp. 445-454.

Raiffa, H. 1968: Decision Analysis, Addison-Wesley, Reading, Massachusetts.

Savage, L.J. 1954. The Foundations of Statistics, Wiley, New York.

Slovic P., B. Fischhoff, and S. Lichtenstein. 1979. Rating the Risks, Environment, Vol. 21, No. 3, pp. 36-39.

Tversky, A. and D. Kahneman. 1974. Judgement Under Uncertainty: Heuristics and Biases, Science, Vol. 185, 27 September, 1974, pp. 1124-1131.

Von Neumann, J. and O. Morgenstern. 1953. Theory of Games and Economic Behavior, Princeton University Press, Princeton, New Jersey.

APPENDIX: REALIZATIONS OF THE DIFFERENT STATE VARIABLES IN MODELS AND DETAILS OF THE ILLUSTRATIVE RESULTS

Figure A1 shows on an influence diagram that was run using Netica software, an example of data for the terrorist decision model with data displayed for the Islamic fundamentalist group. Figure A2 shows on an influence diagram, an example of data for the terrorist decision model in general.

Realizations in the Terrorist decision model shown in Figures 2 and 3, and A1.

Objective: Symbolism and Losses (loss of life)

Group: Islamic Fundamentalist Groups, Islamic Fundamentalist Individuals, American Disgruntled Groups, American Disgruntled Individuals, and Other Foreign Nationals.

Belief about US Response: Protect Government Buildings, Protect Big Cities, Protect All Symbolic Buildings, and Do Nothing.

Material Available: Yes and No

Threat: Nuclear Warhead or Dirty Bomb, Biological, and Conventional

Target: Government Building, Urban Population, Symbolic Building, and Transportation Network

Means of Delivery: Plane, Truck, and Person

Able to Carry out Attack: Yes and No

Belief about Effectiveness of Response: Stops Attack, Lessens the Affect of the Attack, and No Effect on the Impact of the Attack.

Resulting Symbolism: Clear, Mixed, and None.

Loss of Life from the Attack: None (0 deaths), Low (1 - 49 deaths), Medium (50 - 499 deaths), High (500 – 3000 deaths), and Very High (greater than 3000 deaths).

Realizations in the U.S. decision model shown in Figures 2, 3, and A2.

Group Involved: Islamic Fundamentalist Groups, Islamic Fundamentalist Individuals, American Disgruntled Groups, American Disgruntled Individuals, and Other Foreign Nationals.

Attack Planned: Yes and No.

US Intelligence Information: Attack Planned and Attack Not Planned

Means for the Attack Available?: Available and Unavailable

Able to Carry Out the Attack?: Yes and No

U.S. Belief about Terrorist Target: Government Building, Urban Population, Symbolic Building, Transportation Network, and No Attack Planned.

Terrorist Threat Given Attack: Nuclear Warhead or Dirty Bomb, Biological Weapon, and Conventional Explosives.

U.S. Response: Protect Government Buildings, Protect Urban Populations, Protect Symbolic Buildings, and Protect Transportation Networks.

Effectiveness of Response: Stops the Attack, Lessens the Impact of the Attack, and Has No Effect on the Impact of the Attack.

Delivery Means given Attack: Plane, Truck, and person

Resulting Symbolism: Clear, Mixed, and None

Loss of Life from Attack: None (0 deaths), Low (1 - 49 deaths), Medium (50 - 499 deaths), High (500 – 3000 deaths), and Very High (greater than 3000 deaths).

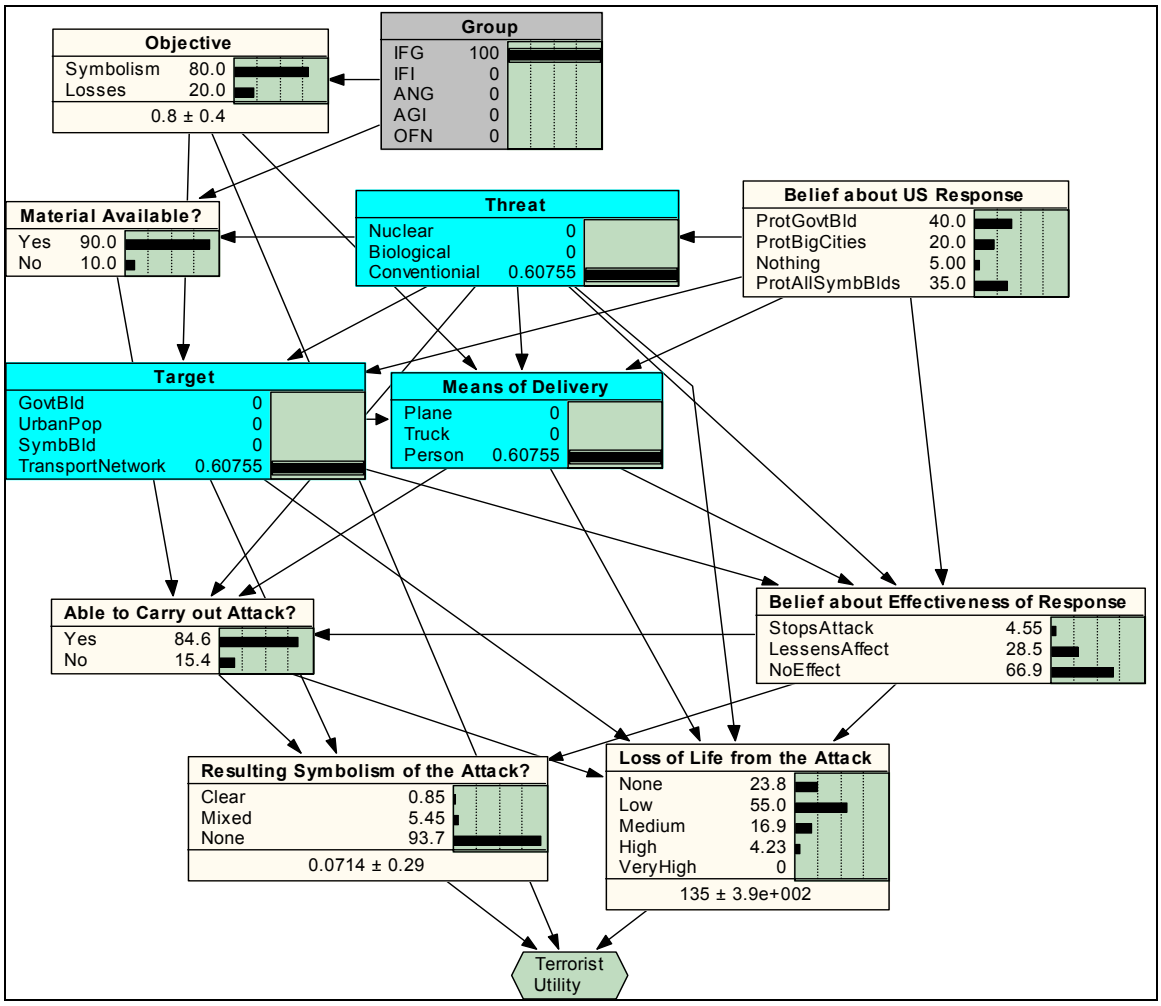


Figure A1: Example of Data for the Terrorist Decision Model with Data Shown for the Islamic Fundamentalist Group.

The resolution of the influence diagram displayed in Figure A1 (uncertainty nodes show probabilities and decision nodes show utilities as a function of the alternatives chosen) shows, for example, that according to our model and for our illustrative data, the expected utility of a conventional attack by person on a transportation network to an Islamic fundamentalist group would be approximately 1.09 computed from the utility function $U(Sy,L) = k_1 Sy + (1-k_1)\log(L)$. Sy is an indicator variable for the symbolism of the attack and is assigned a value of 2 for a clearly symbolic attack, a value of 1 for an attack with mixed symbolism, and a value of 0 for an attack with little or no symbolism. L is the loss of life from the attack. Note that in Figures A1 and A2 the arrow between "Material Available" and "Threat" has been put in the assessment order – opposite the direction it was in Figure 1. This led to a more natural analysis of the data.

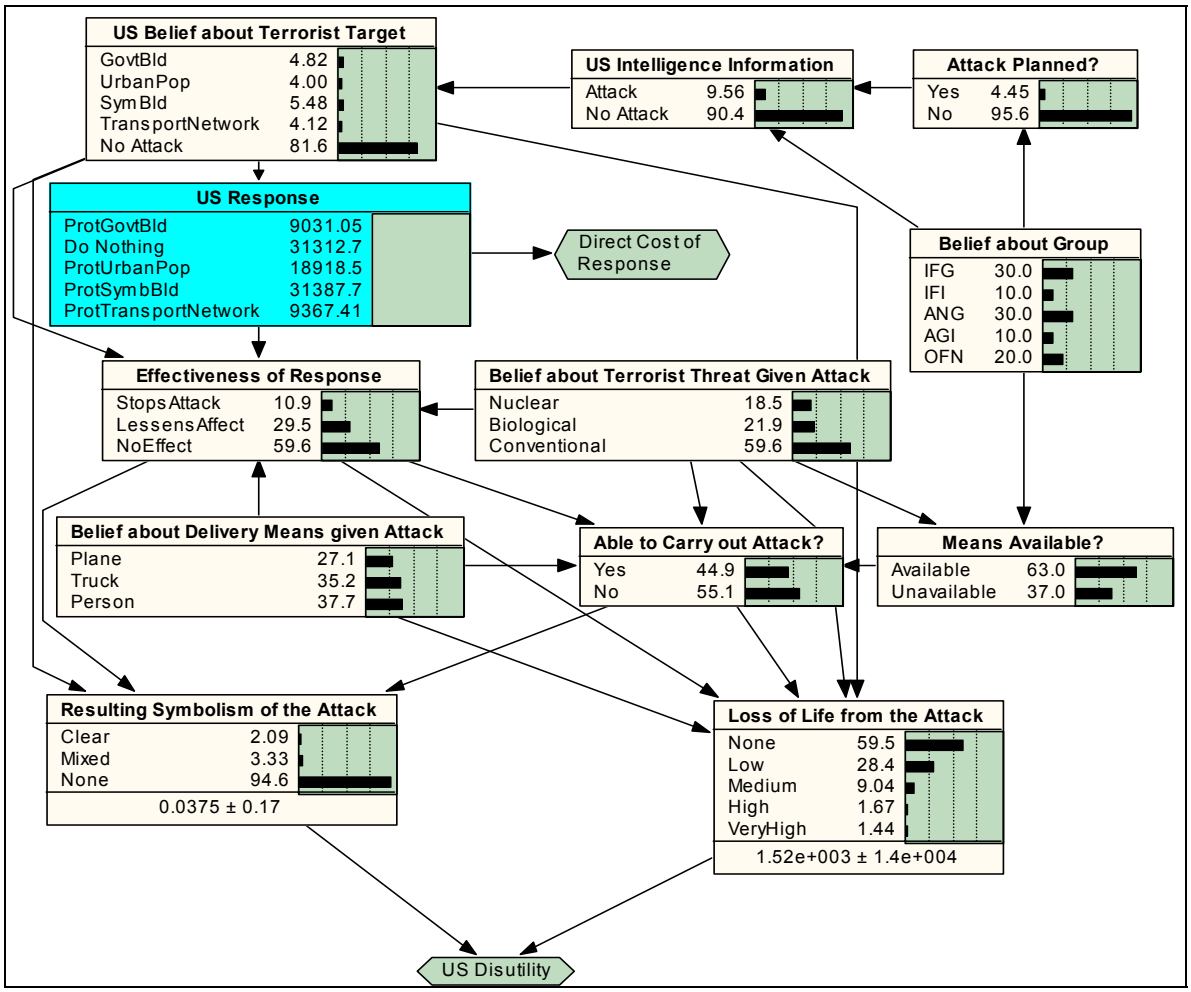


Figure A2. Example Data for the Terrorist Decision Model.

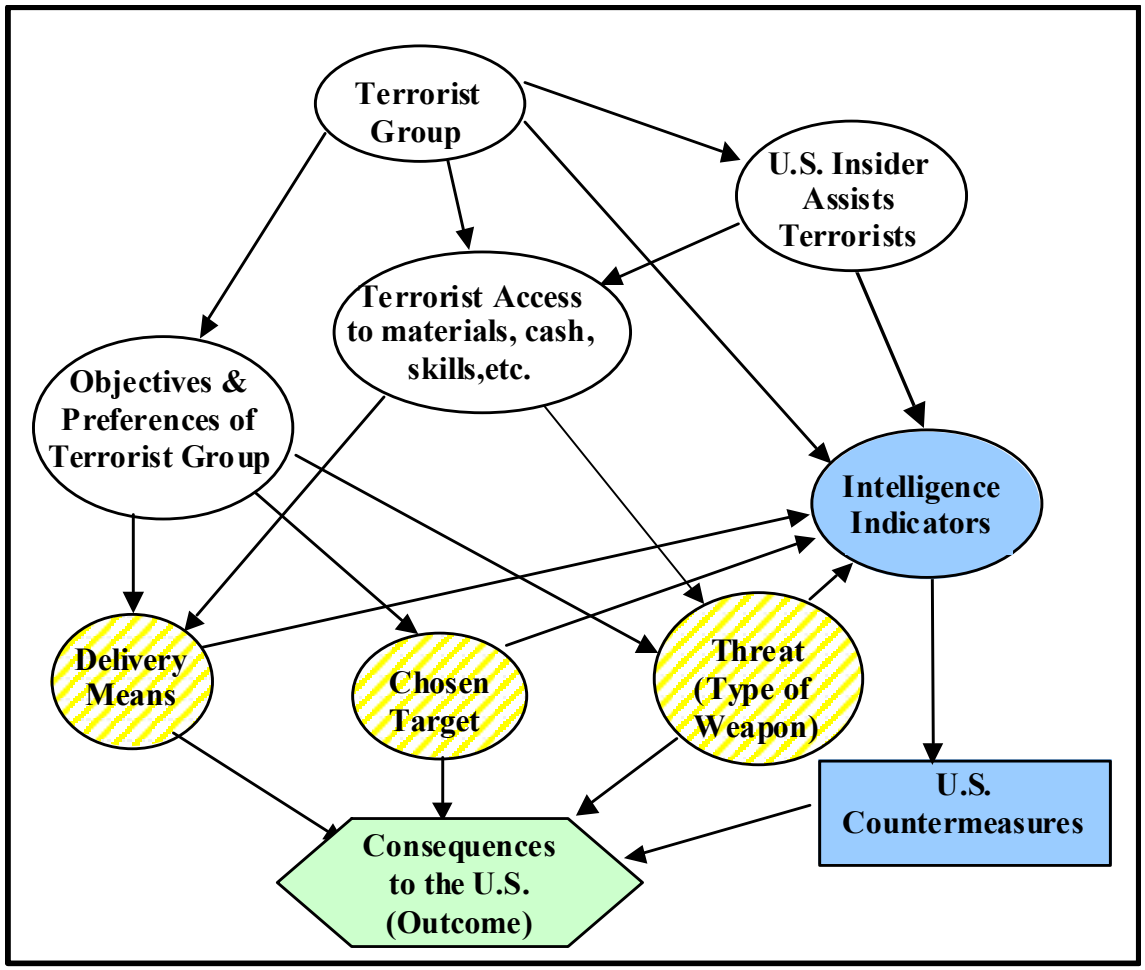
The resolution of the influence diagram displayed in Figure A2 shows, for example, that given the updated beliefs about the probabilities of different terrorists attacks as described in Section 6, the optimal (i.e., disutility minimizing) decision in the relevant time period is to protect government buildings.

Table A1 shows the (joint) probability of occurrence for each of the possible attack scenarios (threat, target, means of delivery) given that an attack is launched. These probabilities are found by using the left side of Figure 2 with the data shown in Figures A1 and A2. The results shown in Table A1 are then used as the input to the right side of Figure 2, the model of the U.S. decision regarding countermeasures.

Table A1. Scenario probabilities per time period conditional on an attack being launched computed from the terrorist decision model.

Target	**Threat**	**Delivery Means**	**Probability**
Government Building	Nuclear	Truck	0.013
Government Building	Nuclear	Plane	0.007
Government Building	Nuclear	Person	0.016
Government Building	Biological	Truck	0.025
Government Building	Biological	Plane	0.018
Government Building	Biological	Person	0.027
Government Building	Conventional	Truck	0.060
Government Building	Conventional	Plane	0.050
Government Building	Conventional	Person	0.060
Urban Population	Nuclear	Truck	0.017
Urban Population	Nuclear	Plane	0.013
Urban Population	Nuclear	Person	0.020
Urban Population	Biological	Truck	0.018
Urban Population	Biological	Plane	0.007
Urban Population	Biological	Person	0.017
Urban Population	Conventional	Truck	0.045
Urban Population	Conventional	Plane	0.035
Urban Population	Conventional	Person	0.049
Symbolic Building	Nuclear	Truck	0.013
Symbolic Building	Nuclear	Plane	0.025
Symbolic Building	Nuclear	Person	0.023
Symbolic Building	Biological	Truck	0.025
Symbolic Building	Biological	Plane	0.024
Symbolic Building	Biological	Person	0.029
Symbolic Building	Conventional	Truck	0.060
Symbolic Building	Conventional	Plane	0.065
Symbolic Building	Conventional	Person	0.061
Transportation Network	Nuclear	Truck	0.020
Transportation Network	Nuclear	Plane	0.001
Transportation Network	Nuclear	Person	0.017
Transportation Network	Biological	Truck	0.013
Transportation Network	Biological	Plane	0.002
Transportation Network	Biological	Person	0.014
Transportation Network	Conventional	Truck	0.042
Transportation Network	Conventional	Plane	0.024
Transportation Network	Conventional	Person	0.044

FIGURES



Legend: Oval nodes: uncertainties about events and random variables. White nodes: uncertainty about terrorist groups and their activities, including (striped) the elements of an attack scenario. Grey nodes: U.S. side. Square node: decision node. Hexagonal node: consequences to the U.S. of an attack scenario given countermeasures. Arrows: probabilistic dependencies

.

Figure 1: Influence diagram representation of an overarching model for the prioritization of threats and countermeasures.

Table 1: Illustrative data and terrorist utility calculation for the basic model

Nature of the threat (weapon)	**Group**	**P_{TE}(Success| Intent [I_j] and weapon [W_i])**	**Attractiveness to perpetrators of successful outcome of W_i**				**Expected utility to the terrorist groups**
			X_1	**X_2**	**X_3**	**Total Utility U_{ij}**	
Nuclear warhead explosion	IF	0.01	10	10	10	30	0.27
	AD	-	-	-	-	-	-
Nuclear incident	IF	0.5	8	3	5	16	5.6
	AD	0.5	4	2	5	11	1.1
Smallpox attack	IF	0.7	2	7	8	17	8.3
	AD	0.6	2	7	8	17	3.1
Continuous conventional attack on urban areas	IF	0.9	4	2	9	15	12.2
	AD	0.9	4	2	9	15	12.2

Legend: X_1 symbolism of the attack, X_2 number of casualties and amount of destruction the caused by the attack, and X_3 degree to which the attack leads to political destabilization and erosion of U.S. power.

Table 2: Illustrative results for the basic model

Probability of intention: $P_{US}(I_1)=0.4$; $P_{US}(I_2)=0.2$; 1:Islamic Fundamentalists. 2:American Disgruntled

Nature of the threat (weapon) W_i	**Group IF: Islamic Fund. Amer. Disgr.**	**Probability of Attack of type i from group j: $P_{TE}(W_i\|I_j)$**	**Probability of success of attack of type i from group j: $P_{US}(S\|W_i,I_j)$**	**Negative value (disutility) of outcome to the U.S. of a successful attack of type i $\underline{U}_{US}(S,W_i)$**	**Expected disutility of a successful attack of type i to the U.S. $E\underline{U}_{US}(S,W_i)$**
Nuclear warhead explosion	IF AD	0.01 -	0.50 -	-10,000	-20
Nuclear incident	IF AD	0.21 0.07	0.20 0.15	-10	-0.18
Smallpox attack	IF AD	0.31 0.19	0.60 0.60	-100	-8.6
Attack on urban areas with conventional weapons	IF AD	0.47 0.74	0.90 0.50	-10	-2.1

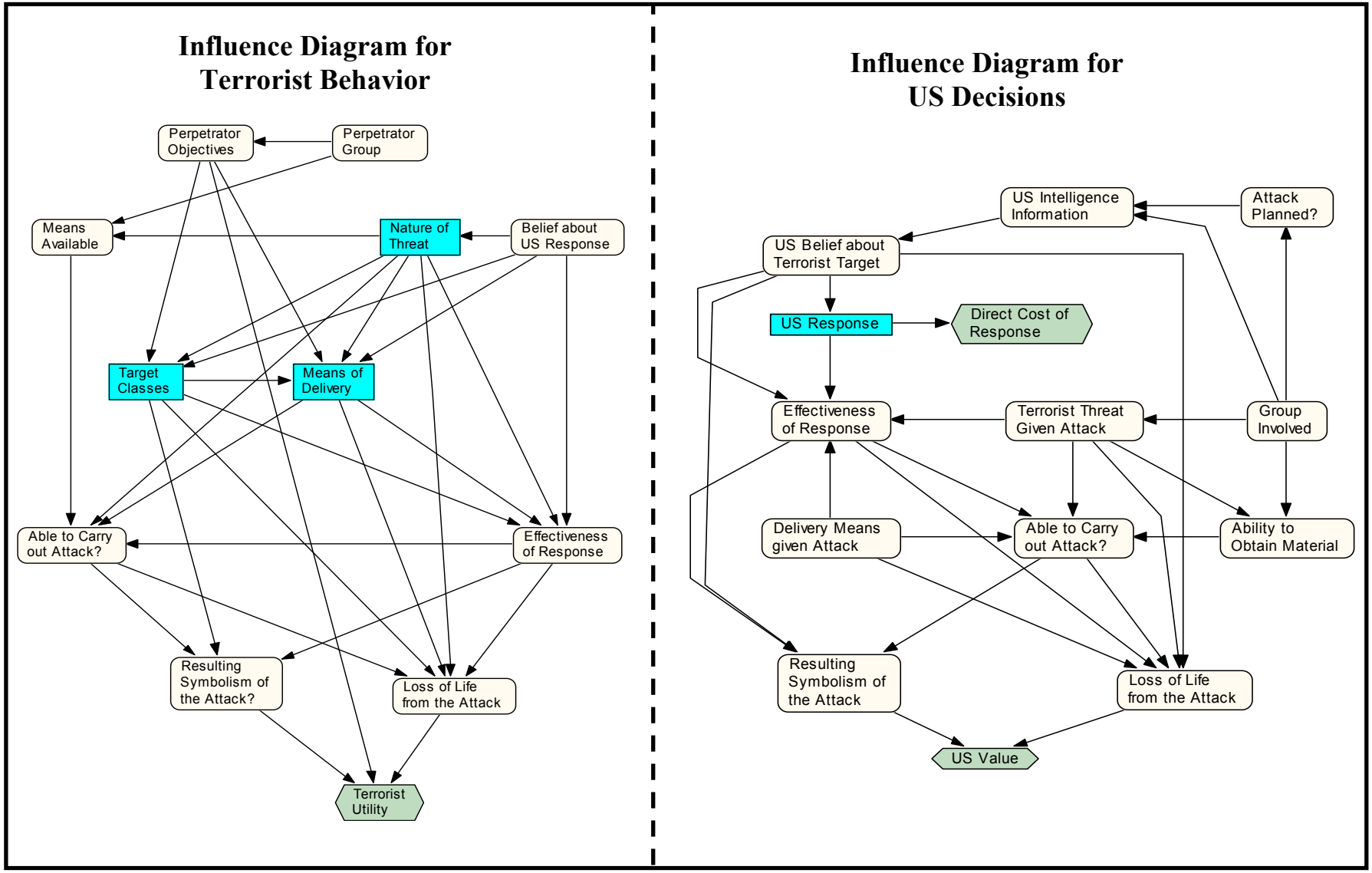


Figure 2. Single-period influence diagrams for the terrorists' and U.S. decisions.

Table 3. Illustrative results for the marginal probabilities of classes of attack scenarios without countermeasures (*status quo*). **Note: these figures are based on fictitious numbers and do not attempt in any way to represent actual beliefs.**

Class of Scenarios	Approximate Probability of Occurrence per time unit
All scenarios involving attack with a nuclear warhead	7.8×10^{-4}
All scenarios involving attack with a biological weapon	9.8×10^{-4}
All scenarios involving attack with conventional explosives	1.9×10^{-3}
All scenarios involving an attack on a government building	1.2×10^{-3}
All scenarios involving an attack on an urban population	6.8×10^{-4}
All scenarios involving an attack on a symbolic building	1.4×10^{-3}
All scenarios involving an attack on a transportation network	4.8×10^{-4}
All attacks made by truck	1.3×10^{-3}
All attacks made by plane	1.0×10^{-3}
All attacks made by individual carriers	1.4×10^{-3}

Table 4: Illustrative results for the expected disutilities of the different classes of scenarios given that each of them is attempted without additional countermeasures (status quo). **Note: these figures are based on fictitious numbers and do not attempt in any way to represent actual beliefs.**

Class of Scenarios	Approximate Expected Disutility to the U.S.
All scenarios involving attack with a nuclear warhead	1.62×10^5
All scenarios involving attack with a biological weapon	2.4×10^3
All scenarios involving attack with conventional explosives	1.4×10^3
All scenarios involving an attack on a government building	3.7×10^4
All scenarios involving an attack on an urban population	3.4×10^4
All scenarios involving an attack on a symbolic building	3.6×10^4
All scenarios involving an attack on a transportation network	3.3×10^4
All attacks made by truck	3.0×10^4
All attacks made by plane	3.0×10^4
All attacks made by individual carriers	3.4×10^4

Table 5. Illustrative Computation of the Expected Disutilities Corresponding to Examples of U.S. Countermeasures. **Note: these figures are based on fictitious numbers and do not attempt, in any way, to represent actual beliefs.**

Countermeasure	**Expected Disutility to the U.S. with the considered measure**
Protect Government Buildings	-9,031
Protect Urban Populations	-18,918
Protect Symbolic Buildings	-9,045
Protect Transportation Networks	-9,367
No Countermeasures	-31,312

Table 6: Illustrative computation of the net benefits of examples of U.S. countermeasures in terms of variation of the probability of a successful attack of each type, given that such an attack is attempted per time unit. **Note: these figures are based on fictitious numbers and do not attempt, in any way, to represent actual beliefs.**

Class of Scenarios	**Conditional Probability of Success per time unit if protecting:**				
	Nothing	**Government Buildings**	**Urban Populations**	**Symbolic Buildings**	**Transpor-tation Networks**
All scenarios involving attack with a nuclear warhead	0.175	0.135	0.164	0.135	0.138
All scenarios involving attack with a biological Weapon	0.180	0.129	0.158	0.121	0.132
All scenarios involving attack with conventional Explosives	0.757	0.523	0.660	0.527	0.536

Table 7: Illustrative computation of the net benefits of examples of U.S. countermeasures in terms of variation of expected disutilities per time unit **Note: these figures are based on fictitious numbers and do not attempt, in any way, to represent actual beliefs.**

Countermeasure	**Decrease in Expected Disutility (Benefits) Relative to not Implementing any Countermeasure (*status quo*)**
Protect Government Buildings	22,282
Protect Urban Population Centers	12,394
Protect Symbolic Buildings	22,265
Protect Transportation Networks	21,945

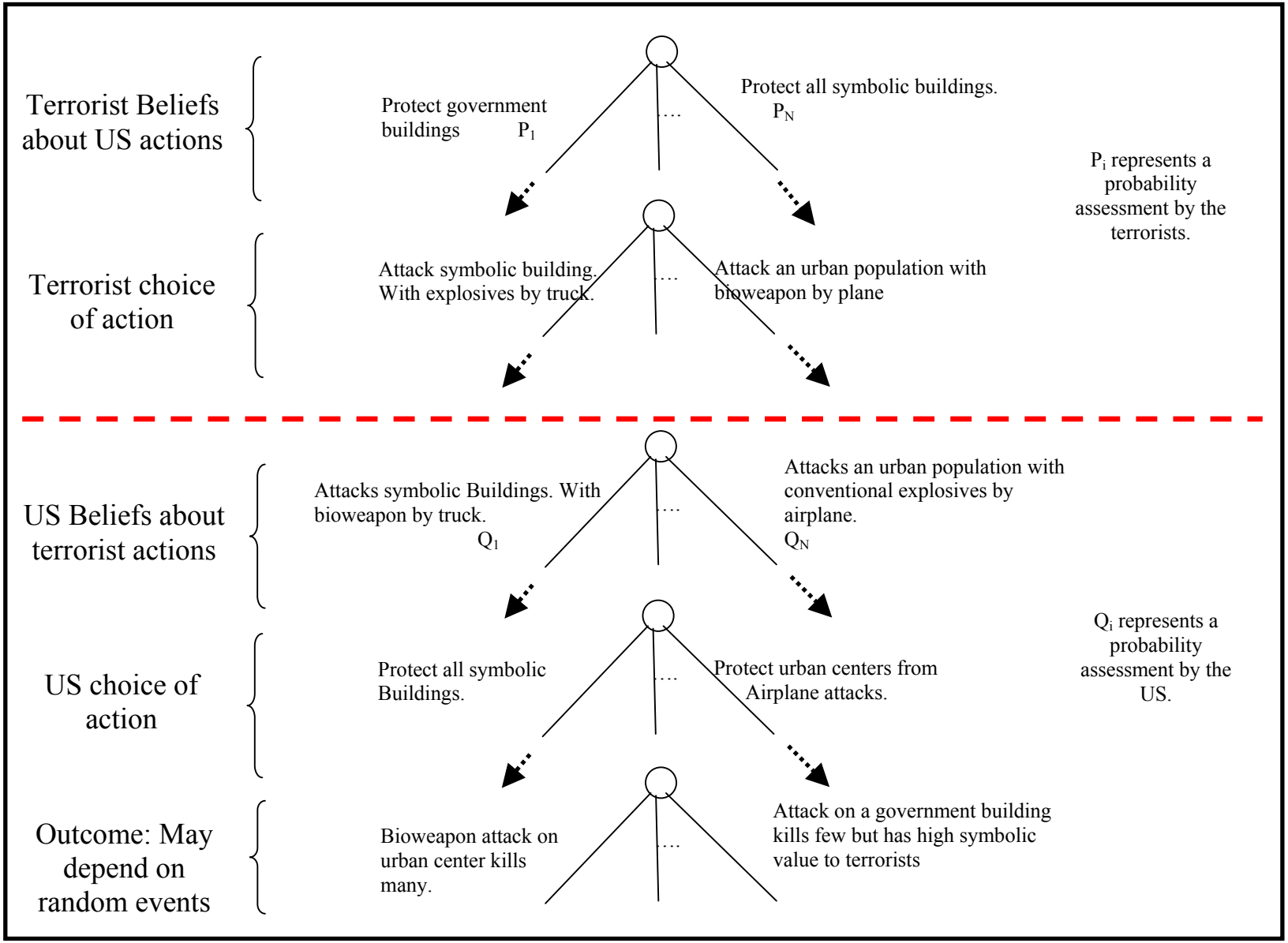


Figure 3. General Game Theoretic Model for the Terrorism Problem.

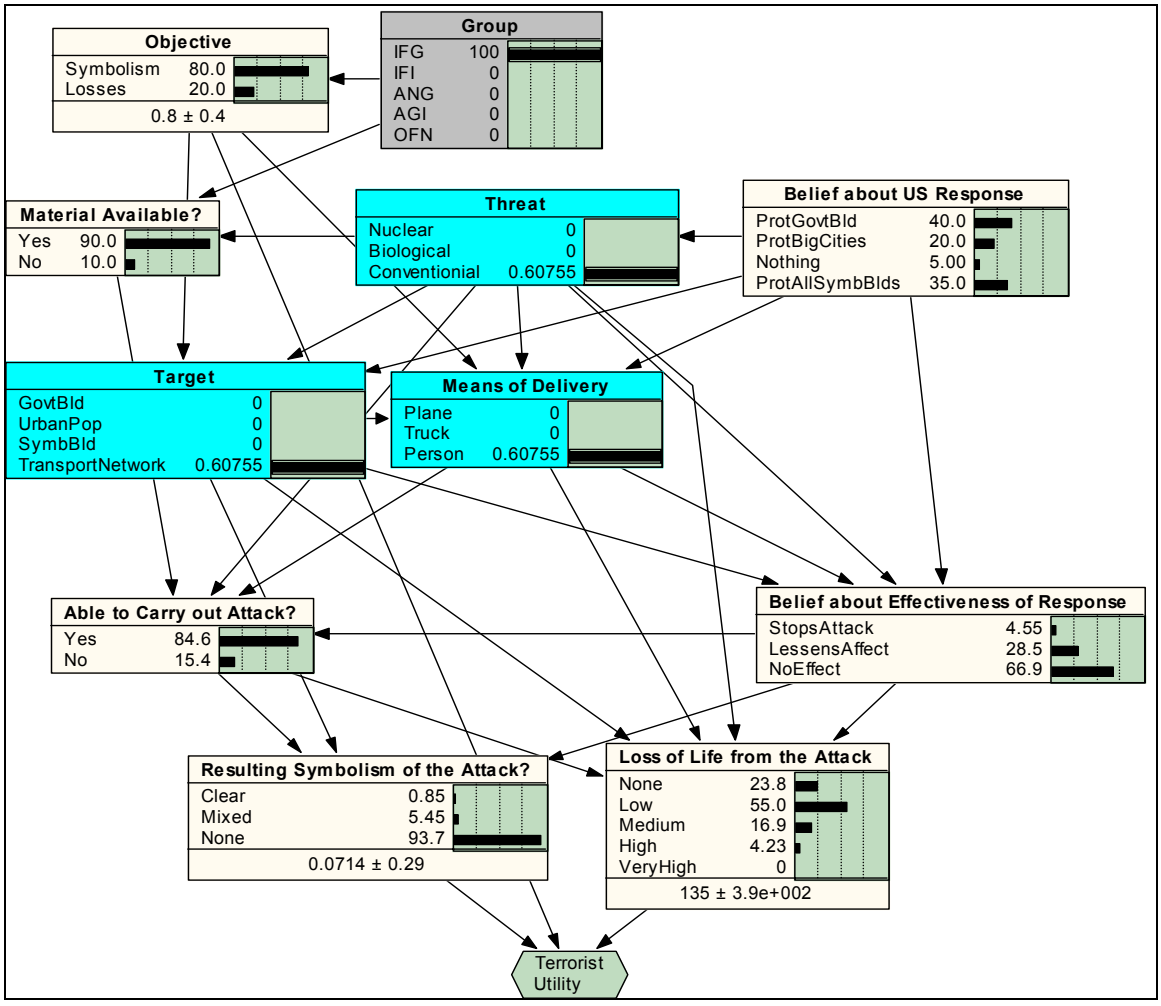


Figure A1: Example of Data for the Terrorist Decision Model with Data Shown for the Islamic Fundamentalist Group.

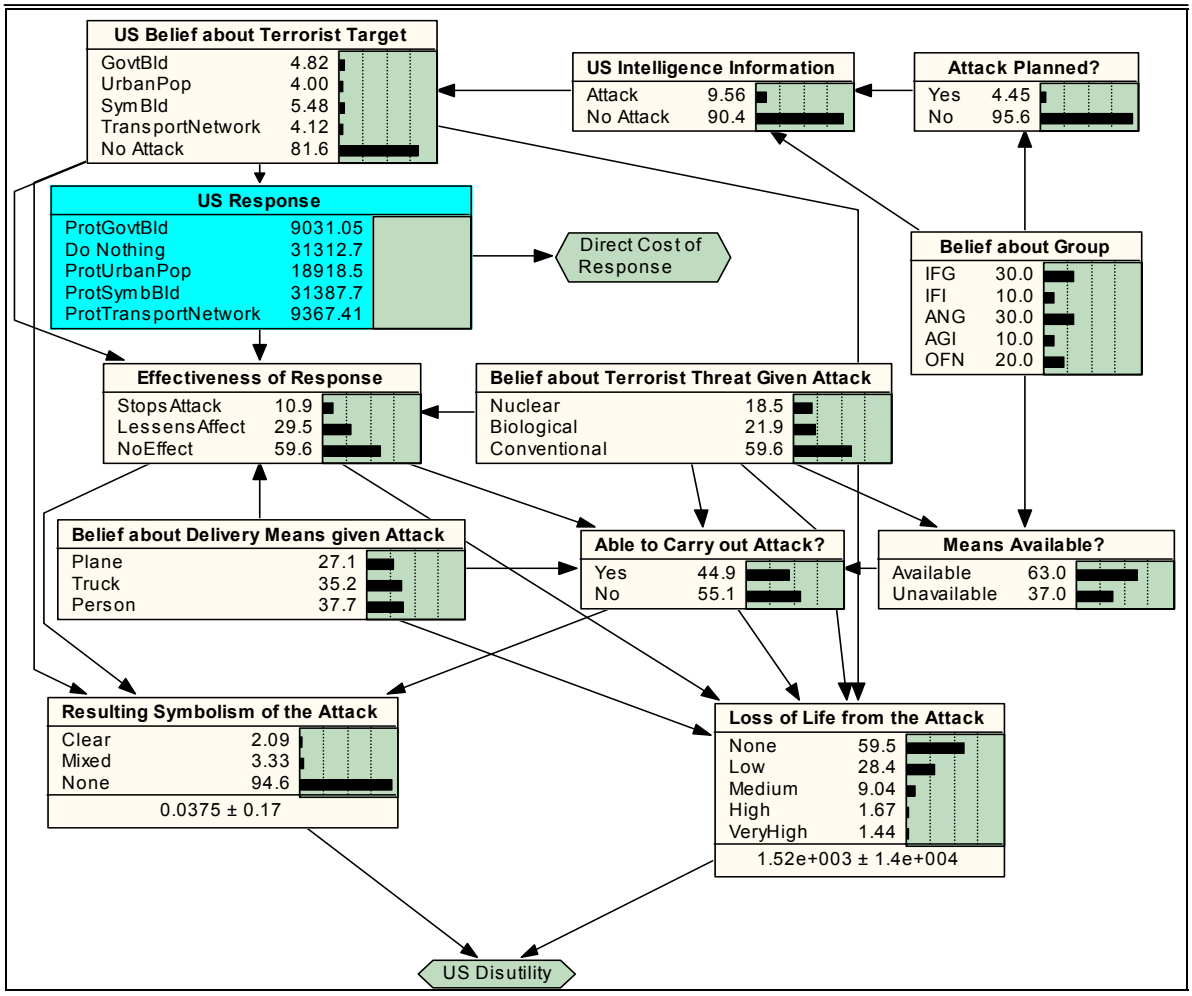


Figure A2. Example Data for the Terrorist Decision Model.