ABSTRACT

Understanding and adapting to an evolving terrorist threat presents a significant challenge to intelligence and law enforcement communities around the world. The goal of this paper is to introduce a new approach to developing dynamic profiles for terrorist organizations to give decision makers a new tool to analyze the evolution of terrorist organizations and estimate the likelihood of future attacks. The proposed method builds on aspects of Bayesian probability and multi-objective decision analysis to adapt to the terrorist threats of the 21st Century. This approach adds to the current literature by proposing a new dynamic structure for assessing and adapting to a constantly changing landscape of terrorist threats, ideologies, and leadership. The proposed method could potentially reduce the time necessary to develop a profile for a terrorist organization, and provide an efficient method of estimating terrorist strategy and impact. These profiles could then be adjusted based on terrorist threats and actions over time. This paper concludes with an example application of the proposed method for a hypothetical terrorist scenario.

INTRODUCTION

The terrorist attacks that happened in the United States on September 11, 2001 (9/11) resulted in almost 3,000 deaths and an international mobilization to counter the growing threat of terrorism from violent extremist groups (Rostow, 2002). Due to the ongoing global threat of attacks by such groups (e.g., bombings in Indonesia, Iraq, Pakistan, and Afghanistan), it is important to identify effective ways of understanding and responding to terrorist threats (Johnson, 2013; Satha-Anand and Urbain, 2013). A wide range of risk and decision analysis methods have become increasingly important tools in the fight against terrorism in an effort to effectively counter terrorism (Willis and Kelly, 2005; Ezell et al., 2010), but the ''War on Terror'' is far from over (Walzer, 2013).

Understanding and adapting to the threat of terrorism poses a significant challenge to intelligence and law enforcement communities worldwide. The task of assessing the risk of an attack is time-intensive and costly, and this task is even more difficult as the composition and objectives of terrorist organizations change. The active pursuit of terrorist organizations by nations around the world has resulted in the death of some terrorist threats (Guiora, 2012); however, terrorist organizations have adapted. Some of the ways that organizations have survived is by changing leadership, finding new sources of funding/support, and operating in smaller cells with more limited communication (Jackson et al., 2005). Events like the Middle East uprisings that started in 2011 (Arango et al., 2012) and the March 2013 assault on a gas refinery in Africa (Trindal, 2013) have highlighted the new capabilities and objectives of active terrorist organizations (Argomaniz, 2013; Ezell et al., 2012).

It is important to understand the motivations and behavior of terrorist organizations in order to effectively counter the threat of terrorist attacks. Understanding the tactics of terrorist organizations is difficult when they are highly adept at survival, and also have changing membership and leadership (Crenshaw, 2000). This paper discusses a new approach to assessing terrorist organizations in a dynamic environment. We propose a quantitative method for terrorist threat assessment based on expert assessment and organizational behavior. The proposed method could potentially reduce the time necessary to develop a profile for a terrorist organization, and provide an efficient method of estimating terrorist strategy and impact.

BACKGROUND

One of the key challenges of counterterrorism operations is that the exact motivations and tactics of a terrorist group are often unknown. Additionally, over time terrorist organizations do learn and change to survive, grow, and improve (Jackson et al., 2005). In this paper, we propose an approach to risk analysis that uses a set of potential terrorist objectives to provide a flexible method for understanding new and changing terrorist organizations, and the threat posed by such organizations.

Developing Profiles of Terrorist Organizations

The task of analyzing a single terrorist organization is time-consuming and involves aggregating information from many

Introducing Terrorist Archetypes: Using Terrorist Objectives and Behavior to Predict New, Complex, and Changing Threats

John Coles

CUBRC
john.coles@cubrc.org

Jun Zhuang

University at Buffalo
jzhuang@buffalo.edu

APPLICATION AREAS:
Threat Assessment and Countermeasures; Irregular Warfare; Decision Analysis

OR METHODOLOGIES:
Pattern Recognition, Multivariate Analysis, Stochastic Processes

sources with varying degrees of reliability (Cronin, 2006; Cox, 2008). Civilian and military personnel working in security and intelligence are constantly faced with complex and fast-paced decisions that impact national security. These decision makers face high-risk scenarios involving threat detection and resource allocation that require vigilance and accuracy. A great deal of work has been done to assess and identify common characteristics of individuals involved in a terrorist organization to help identify potential threats (Russell and Miller, 1977). These organizations have also been profiled based on structure and connectivity to provide insight into how to better defend against potential attacks (Alexander and Swetnam, 2001; Mishal and Rosenthal, 2005; Insua et al., 2009; Medina, 2014). Finally, there have been efforts to develop models for terrorist organizations using contextual and historical information (Faria, 2012). Though profiling terrorist groups may provide some insight into the general behavior of an organization, as far as the authors are aware dynamic profiles have not previously been incorporated into a model for estimating future terrorist behavior.

There are several possible models for how to categorize terrorist actions suggested in the literature (Post, 1984, 1986; Post et al., 2002; Victoroff, 2005). In this paper, we use a wide set of behavior categories to provide a general framework for the proposed method.

- *Attack vector*: The attack vector is the method of attack used in a terrorist action. Some examples are suicide bomb, car bomb, package bomb, improvised nuclear device, radiological bomb, and biological attack.
- *Target type*: The intended target of the attack is an important characteristic of a terrorist organization. Some examples of potential target types are civilian infrastructure, military infrastructure, civilian personnel, military personnel, and security personnel.
- *General features*: The overall behavioral characteristics of a terrorist organization will provide an additional source of insight when attempting to update terrorist profiles. Some examples of organizational behavior are announcing attacks prior, claiming credit for attacks afterwards, and religious emphasis.

Adapting to Terrorist Behavior

One common method for updating a terrorist profile or behavior estimate is using Bayesian probability (Insua et al., 2009; Wang and Bier, 2011). For example, Pate-Cornell and Guikema (2002) incorporated Bayesian updating when considering the probability of success for a particular terrorist or countermeasure, but did not account for adaptive or unknown/misunderstood attackers, something that is of critical importance in defense against terrorism (Cardoso and Diniz, 2009). Pate-Cornell and Guikema (2002) also looked at the potential threat posed by multiple groups, and how those threats could be aggregated using Bayesian probability to generate a single threat score for each potential avenue of attack.

Guikema and Aven (2010) expanded on the Pate-Cornell and Guikema (2002) model by proposing a three-tiered ranking system for threat classification. However, this system only identified extreme situations (tolerable risk and unacceptable risk), putting complex and nuanced threats into a middle category for additional study. Terrorist acts may not appear to be consistent over a period of time for a variety of reasons (e.g., the composition of the group changes, or the goals of the group solidify). As pointed out in the literature (Brown and Cox, 2011; Golany et al., 2009), some limitations of probabilistic modeling remain because ''terrorists do not act randomly.'' In this paper we propose a flexible framework for assessing terrorist organizations that accounts for changing composition and objectives when calculating the likelihood of future actions.

Decision with Multiple Criteria

Multi-objective decision analysis (MODA) and multicriteria decision making (MCDM) are approaches to decision making and optimization that acknowledge the complexity and multifaceted nature of decision making in real-world problems (Triantaphyllou and Baig, 2005). In this paper, we refer to these two fields under the umbrella of MODA for the sake of clarity. One important aspect of this discussion is the idea of model adaptation to a changing terrorist organization. In the broader MODA context, it is important to identify the nuanced objectives of

a stakeholder when they are confronted with a wide array of conflicting objectives.

Counterterrorism is a well-studied topic in the MODA literature (Keeney, 2007; Linkov et al., 2007). However, the relative scarcity of empirical data on terrorist attacks makes it difficult to apply conventional statistical methods (Brown and Cox, 2011). Keeney and von Winterfeldt (1989) provide a good discussion of some of the challenges and solutions that arise when experts are used to assess complex problems. In this paper, we propose a statistical framework that accounts for terrorist attacks, but also includes other observable behaviors or actions.

The process of eliciting the preferences of a decision maker is discussed extensively in the literature and there are a wide variety of possible solutions proposed (Ribeiro, 1996; Chen and Pu, 2004; Wallenius et al., 2008). In the MODA literature, there are several methods proposed to deal with stakeholders whose preferences are inconsistent in the course of the elicitation process (e.g., Zionts and Wallenius, 1976; Yu et al., 1985; Cohon, 2004). Since here we are focusing on terrorist organizations that can change, it is important to consider mechanisms that can adapt to changing or inconsistent behavior. Though there are many different and nuanced MODA approaches that could be discussed (see Belton and Stewart, 2002, for a comprehensive overview), in this paper we build on theory from the MODA literature in two ways.

The first way that we build on the MODA literature is using several of the techniques proposed by Zionts and Wallenius (1976) to find a decision maker's preferences. The method proposed by Zionts and Wallenius used stakeholder preferences to alter a set of weights (λ_i) to find the best decision based on a series of questions about preference. The set of λ_i weights was used to provide a ranked set of decision alternatives based on the decision maker preferences (Zionts and Wallenius, 1976, 1983). Each decision alternative has desirable and undesirable characteristics, which were compared to identify the decision combination that best matched the stakeholder preferences. In the Zionts and Wallenius method, the modeler poses a series of questions to the decision makers to directly compare decision alternatives. With each question, the modeler would add a new constraint and resolve the optimization problem to identify the stakeholder preference region. As the number of questions increased, the size of the decision space diminished if the answer was consistent with previous question responses. This process continued until the decision space was reduced to a small enough region to provide the stakeholder with a clear solution.

In this paper, we use portions of Zionts and Wallenius' method to develop a nuanced profile of a terrorist organization, where each action by a terrorist organization is treated like a response to a question. With each action, the weighting scheme is changed using Bayesian updating instead of adding a new constraint. By updating the weighting scheme directly instead of adding constraints, we keep the decision space open to allow for shifts in an organization's goals. The exact application is discussed in detail in the following section.

The second way that we build on MODA literature is the use of stakeholder elicitation techniques to construct decision alternatives or *archetypes.* In a classical MODA problem, we might have several discrete decision alternatives to choose from, and each alternative has positive and negative characteristics. For example, if a decision maker is choosing a vehicle to purchase, statistics provided about each option might include miles per gallon, horsepower, and interior. To find rankings for each of these characteristics, the stakeholders would provide rankings for each vehicle in the pertinent categories. In this paper, we use stakeholder assessments of terrorist organizations/objectives to help construct archetypes as the decision alternatives. Each archetype has a set of likelihood rankings for each action that a terrorist organization might exhibit (e.g., suicide bombing, pre-attack announcement). The stakeholder elicitation could be done using any proven weight elicitation techniques in the literature (see examples, discussion, and comparison in Gregory and Keeney, 1994; Bottomley and Doyle, 2001; Riabacke et al., 2009).

PROPOSED METHOD

An *archetype* is a set of weights for potential actions that are associated with

a motivation or objective. Archetypes can be combined with other archetypes to describe nuanced motivations and behavior. An archetype is not meant to represent any particular group; rather it is designed to capture some of the common characteristics across a set of terrorist groups. A *profile* for a particular terrorist agency could be developed directly, or as a combination of different archetypes. The development and mixing of terrorist archetypes would provide decision makers a clearer picture of terrorist behavior and motivation.

The terrorist archetypes would be developed with input from stakeholders (e.g., government agencies, politicians, sociologists, experts in counterterrorism) to provide a weighted rank of terrorist priorities and objectives. This input could be elicited using any of the methods discussed in the MODA and expert elicitation literature that provides a single score/number for each characteristic (e.g., Dalton et al., 2010) as discussed in the literature review. Each archetype would be representative of an extremist objective or system of behavior (e.g., a radical organization attempting to remove a foreign influence from a specific country or region, or anarchists/separatists inside a country). Once the individual archetypes are developed by the expert groups, the archetypes could be combined into a single adaptive profile to account for complex terrorist behavior and evolution, rather than attempting to assign specific risk values for each terrorist organization.

Definitions, Notation, and Assumptions

The method proposed in this paper builds on counterterrorism literature but we clarify terminology that is specific to this paper. When defining the terminology we reference MODA terms to provide the reader with additional context. Then we present the set of notation that will be used in this paper. Finally, there are a few key assumptions that are used in the process of developing the archetypes that are important to state. The set of assumptions provides additional perspective on how to structure and apply the proposed method.

Term Definitions.

- *Terrorist/attacker*: A nonstate actor, or affiliated set of actors, that presents an ongoing, tangible threat to vital interests or national security. In this paper, we focus primarily on attackers that exhibit terrorist-like behavior. In MODA terminology, the attacker is the decision maker in the Zionts and Wallenius (1976) method.
- *Action/behavior*: An observable or measurable event (e.g., bombing, kidnapping, making announcement, making threat) that occurs as the result of an attacker's existence or pursuit of specific goals, and that are of interest to the counterterrorism community. In MODA terminology, the action is a characteristic of a decision alternative.
- *Objective*: A single defined goal that an attacker might want to achieve.
- *Objective archetype*: A list of weights for each possible action that an attacker might exhibit when attempting to achieve a single objective. In MODA terminology, the archetype is a vector of values/weights for all the characteristics of a decision alternative
- *Archetype weight vector*: A set of weights for the objectives that an attacking agency might be attempting to achieve. In MODA terminology, the archetype weight vector is a normalized ranking of the decision alternatives
- *Behavior profile*: The likelihood that an attacking agency might exhibit one of the observable actions

Mathematical Notation.

- m: The number of actions attributed to the attacker over time.
- n: The number of different actions that can be taken/demonstrated by the attacker.
- t: The number of archetypes available for defining the attacker profile.
- D: Set of actions that could be taken by an attacker, $D \equiv \{d: d = 1, 2, \ldots, n\}$.
- J: Set of actions attributed to an attacker in chronological order, $J \equiv \{j: j = 0, 1, \ldots, m\}$. The index j is initialized at 0 before any action has been observed.
- $u_{j,d} \in \{0,1\}$: $u_{j,d}$ is the indicator for the type of action d taken in time step j. Only one action can be taken per time step such that $\sum_{d=1}^{n} u_{j,d} = 1 \ \forall j \in J$.

- K: Set of archetypes that are available to describe the attacker, $K \equiv \{k: k = 1, 2, \ldots, t\}$.
- $\alpha \in [0,1]$: Rate of adaption to failure. If an attacker fails at performing an attempted action then this rate allows there to be a different rate of organizational change.
- $x \in [0,1]$: Rate of organizational change. Can be used to slow down or accelerate the shift in organizational objectives.
- $s_j \in \{0,1\}$: Indicator function for whether or not an action was successful; $s_j = 0$ means that attacker failed when attempting an action, and $s_j = 1$ means the attacker was successful at time step j.
- $r_{k,d} \in [0, 1]$: Likelihood that an attacker with the objective of archetype k will display action d; $r_{k,d} = \mathrm{P}(d|k)$.
- $\beta_{d,j} \in [0, 1]$: Likelihood of an attacker taking action d after observing the jth action; $\beta_{d,j} = \mathrm{P}(d|j)$.
- $\lambda_{k,j} \in [0, 1]$: Component of attacker behavior that be described by archetype k after observing the jth action; $\lambda_{k,j} = \mathrm{P}(k|j)$ and $\sum_{k=1}^{t} \lambda_{k,j} = 1 \ \forall j \geq 1$.
- $\boldsymbol{r_k} = (r_{k,1}, r_{k,2}, \ldots, r_{k,n})$: Vector of likelihood estimates for different actions for archetype k.
- $\boldsymbol{\lambda_j} = (\lambda_{1,j}, \lambda_{2,j}, \ldots, \lambda_{t,j})$: Attacker archetype weight vector after the jth action.
- $\boldsymbol{\beta_j} = (\beta_{1,j}, \beta_{2,j}, \ldots, \beta_{n,j})$: Attacker behavior profile vector after the jth action.

Model Assumptions.

1. Terrorist organizations have an objective, or set of objectives, that they are attempting to achieve (Golany et al., 2009; Brown and Cox, 2011).
2. Terrorist actions are executed in an effort to achieve the objective(s) of the organization (Golany et al., 2009; Brown and Cox, 2011).
3. Changes in an organization's objectives will be reflected in the behavior of the organization. This is a natural extension of assumptions 1 and 2 as follows: If an organization has a set of objectives, and acts in such a way to achieve those objectives, then when the objectives of the organization change, the actions the organization exhibits must also change to match the new objectives. This assumption does not hold when different objectives have identical action sets.
4. Actions that can be correctly attributed to a terrorist organization provide insight into that organization's motivations. This follows from assumption 3 that if an organization changes its behavior to reflect different objectives, then the objectives could be gleaned from the organization's actions. In this paper, we propose a dynamic approach to assessing terrorist organizations that uses what is known to continuously improve any initial estimate, so as the terrorist organization acts these actions can be used to improve our understanding of the organization's objectives.
5. Expert elicitation can provide an initial estimate of some of the actions that a terrorist might exhibit when attempting to achieve a particular objective, but are not expected to predict a particular terrorist organization's objectives.

Archetype Methodology

The archetype concept is useful for isolating a single terrorist objective and pairing that objective with a set of associated actions. Archetype development should be conducted in close partnership with a set of decision makers and experts in counterterrorism (stakeholders). In this paper, we use terrorist objectives to develop archetypes and leave other methods for future work, though other potential applications of the framework may be mentioned as examples in passing.

Choosing Archetypes. The first step in archetype development is the selection of a set of objectives that sufficiently captures the threats that will be quantified in the proposed system. If the agency considering threats is the United States government, then the set of objectives used to develop archetypes would include potential threats to US interests and allies. The range of objectives should include innocuous and violent actions to help maximize the chance of effectively classifying the type of threat presented.

When developing archetypes, it is important that the purpose described is not too specific or too general. Example objectives that could be used to develop an archetype include: ''End Protestant rule of Ireland at any cost,'' or

''End US intervention in Egypt through political means.'' Actions by organizations with these archetypes could include things like assassinations, bombings, armed rebellion, and organized protests. It is important to note that all observable behavior by a potential terrorist organization may be useful in assessing potential future threats.

If a purpose is too specific, it may not be applicable at all to the current set of terrorist threats. An example of an archetype that might be too specific is ''End US intervention in Egypt by manipulating the 2012 presidential elections.'' While this objective may be pertinent in the short-term, an archetype with such a narrow objective will not be useful when attempting to assess future threats. Conversely, an archetype that is too general (e.g., ''Destroy France'') may not be very useful in understanding or defining changing threats.

A different approach to archetype development might encourage stakeholders to treat some of the better known terrorist organizations as unique archetypes. The advantage of this approach is that it would likely reduce the amount of time required to identify and develop archetypes. However, one of the key disadvantages of using well-known terror organizations to form the basis of the archetype methodology is that the framework could rapidly become outdated. Another challenge is that it may be difficult (and potentially confusing) to describe new terrorist organizations as a combination of older organizations, especially if those organizations no longer exist. This method of archetype development may also add too much specificity in the archetype definition and would be less reliable as the older organizations that served as a basis for the original archetypes change.

Developing an Archetype. The next step in the archetype development process is the identification of terrorist actions that should be monitored. With the list of objectives found using the methods discussed in previous sections, the stakeholders would estimate the likelihood of actions for each archetype. Participants in the elicitation process would be asked to estimate the likelihood that a group with objective k would attempt action d. For every archetype the stakeholders would work to assign likelihood estimates for each possible action. In MODA terminology, the participants would be asked to provide the values of the characteristics of each decision alternative to be considered. The product of the elicitation process would be a set of $\boldsymbol{r_k}$ vectors for each of the k archetypes. A fully elicited archetype would be put into a format similar to Table 1, with values like those shown in the example application (Table 4). In future iterations and applications of this model, it may be appropriate to recommend a specific approach to eliciting the weights used in the archetype. However, for the purpose of this paper we focus on developing the broad approach, rather than specifying an elicitation technique.

Combining Archetypes into a Terrorist Profile. In the proposed method, archetypes serve as the basic building block for analyzing and understanding the behavior of terrorist organizations. The next step in the archetype process is to build profile vectors, $\boldsymbol{\lambda_j}$, from the individual archetypes developed using expert elicitation (see the previous subsection). In this section, we define the mechanism for developing a terrorist profile vector from terrorist archetypes, and then introduce several techniques that could be used to develop an initial attacker profile using archetypes. An archetype weighting vector framework is shown in Table 2.

The archetype weights can be written simply as a sequence of weights $\lambda_{k,j}$ in a vector ($\boldsymbol{\lambda_j}$). It is important to develop profiles that are meaningful and provide specific enough

Table 1. Objective archetype vector.

Category	Attack vector	Attack target	General features
Name	Behavior 1 …	Behavior d …	… Behavior n
Archetype k	$r_{k,1}$ …	$r_{k,d}$ …	… $r_{k,n}$

Note: An example archetype with different behaviors (d) will be scored by the stakeholders.

Table 2. Archetype weight vector.

Name	Archetype 1	Archetype k	Archetype t
Terrorist organization	$\lambda_{1,j}$	$\lambda_{k,j}$	$\lambda_{t,j}$

Note: To combine several archetypes into a single terrorist profile, we give weights to each archetype. In this table we look at an archetype weight vector with a value ($\lambda_{k,j}$) assigned to each archetype after the jth action.

estimates of terrorist behavior such that stakeholders can make decisions about how to engage with a particular organization. However, though initial profiles should capture key features of the organization, the definition of the attacking organization should remain broad enough to account for ''new,'' or previously unobserved, actions. Here we provide some examples of how an initial terrorist profile could be constructed from a set of archetypes, motivated by the work of Zionts and Wallenius (1976). It should be noted that for all $\lambda_{k,j}$ discussed here, $j = 0$ since we assume that the framework for assessing a terrorist organization is set before accounting for any recent actions by the attacker.

- *Focused*: Start with a single objective k, and give all the weight to that particular archetype ($\lambda_{k,0} = 1$; $\lambda_{1,0} = \lambda_{2,0} = \ldots = \lambda_{k\text{-}1,0} = \lambda_{k+1,0} = \ldots = \lambda_{t,0} = 0$). This strategy would be appropriate if a terrorist organization appears to be entirely focused on a single objective without regard to any others. The advantage of this method is that it would provide a clear and quick estimate for what type of behaviors an organization might exhibit. However, the drawback of such a simple initial construction is that it may provide an overly confident estimate of future action and take longer to identify other objectives that were initially obscured.
- *Generalist*: Start with an equal weighting for all objectives (say all archetypes, t) that a terrorist organization has previously claimed, or that stakeholders believe may be driving the organization ($\lambda_{1,0} = \lambda_{2,0} = \ldots = \lambda_{t,0} = 1/t$). Then, as the terrorist organization exhibits different behaviors over time, the profile will be updated according to the methods to be discussed previously. The advantage of this tactic is that stakeholders will not be very surprised if a terrorist organization exhibits behaviors that haven't previously been observed. The disadvantage of this approach is that if the initial list of objectives attributed to a terrorist organization is very disparate, it may be challenging to easily identify what behaviors the terrorist organization is most likely to exhibit in the future.
- *Adapted*: Start with one of the two approaches described above (1 or 2). Then update the terrorist profile to the present time using the historical behavior of the terrorist organization to start identifying what the current terrorist profile might look like. The advantage of this approach is that stakeholders will be able to use a nuanced behavioral profile in the future. However, it is important to note that there is a significant danger of confirmation bias if this approach is used because the initial set of archetypes chosen by the stakeholders to represent the terrorist organization would have been informed by the historical behavior. Thus, using the historical behavior to update the terrorist profile may just reinforce the stakeholders' perception of the terrorist organization and provide a biased estimate of future behavior.
- *Stakeholder*: Start with a set of objectives that the terrorist has claimed, and have stakeholders select the initial weights assigned to each archetype (normalized such that $\sum_{k=1}^{t} \lambda_{k,0} = 1$). The advantage of this approach is that it is a quick method to generate a nuanced profile of a terrorist organization. The disadvantage of this method is clear since there is a significant source of bias introduced into the method, which may reduce the reliability of the proposed approach and take a long time for the method to self-correct as the terrorist organization acts.

The approaches listed here are stakeholder driven, but in future work we will examine

what other techniques could be used to define a starting profile for a terrorist organization. For example, by examining the set of behaviors that a terrorist organization has exhibited historically, one could generate a starting profile for the terrorist organization and reverse engineer archetype combinations for the profile. This method will provide a precise estimate based on exhibited behaviors, but could generate a large number of archetype combinations that might fit the exhibited behaviors if the archetypes are not linearly independent. Thus, this method might still require stakeholder intervention to identify the most likely initial archetype combination to represent a terrorist organization.

Similarly, the behavioral profile can be written as a sequence of characteristics that the organization is likely to exhibit as a vector $\boldsymbol{\beta_j} = (\beta_{1,j}, \beta_{2,j}, \ldots, \beta_{n,j})$. The behavioral profile is calculated using the values from Tables 1 and 2 as shown in Equation 1. This calculation provides an initial estimate of the likelihood observing each possible action as seen in Table 3. The calculation shown in Equation 1 is done every time the terrorist acts ($j \in J$), for the set of possible actions ($d \in D$).

$$\beta_{d,j} = \sum_{k=1}^{t} \lambda_{k,j} r_{k,d} \quad \forall\, d \in D \tag{1}$$

Updating the Attacker Profile. Once an initial profile has been formed, it is important to have a clear methodology for updating the profile as new information becomes available. In this paper, we use Bayesian probability to update the archetype weighting vector $\boldsymbol{\lambda_j}$ after the jth action is observed. To develop the concept clearly, we start with Bayes Rule to find P($k|d$), the portion of terrorist behavior that can explained by archetype k after the jth action of type d.

$$\mathrm{P}(k|d) = \frac{\mathrm{P}(d|k)\mathrm{P}(k)}{\mathrm{P}(d)} = \frac{\mathrm{P}(d|k)\mathrm{P}(k)}{\sum_{k=1}^{t} \mathrm{P}(d|k)\mathrm{P}(k)} = \frac{r_{k,d}\lambda_{k,j-1}}{\sum_{k=1}^{t} r_{k,d}\,\lambda_{k,j-1}} \forall\, k \in [1,t] \tag{2}$$

$$\lambda_{k,j} = \mathrm{P}(k|d) = \frac{r_{k,d}\lambda_{k,j-1}}{\sum_{k=1}^{t} r_{k,d}\,\lambda_{k,j-1}} \forall\, k \in [1,t] \tag{3}$$

By expanding on Bayes rule in Equation 2, we can derive Equation 3 to update the components of the weight vector $\boldsymbol{\lambda_j}$, after observing the jth action of type d. Equation 1 is then applied to find the behavior vector $\boldsymbol{B_j}$. Since each terrorist organization is different, it is important to incorporate control parameters that alter the updating process. In this paper we propose two control variables that could be used to update the vector $\boldsymbol{\lambda_j}$ after an action is observed: Rate of adaption to failure (α) and Rate of organizational change (x). In Equations 4 (probability) and 5 (weights) the control variables α and x are added see how the information gained using Bayes rule (Equation 2) could be applied to account for differences between terrorist organizations.

$$\lambda_{k,j} = \mathrm{P}(k) + x\big(1 - \alpha\big(1 - \mathrm{s}_j\big)\big) \times (\mathrm{P}(k|d) - \mathrm{P}(k)) \,\forall\, k \in [1,t] \tag{4}$$

$$\lambda_{k,j} = \lambda_{k,j-1} + x\big(1 - \alpha\big(1 - \mathrm{s}_j\big)\big) \times \left(\frac{r_{k,d}\lambda_{k,j-1}}{\sum_{k=1}^{t} r_{k,d}\,\lambda_{k,j-1}} - \lambda_{k,j-1}\right) \forall\, k \in [1,t] \tag{5}$$

It is important that any updating method used to assess terrorist threats also accounts for

Table 3. Attacker behavior profile.

Category	Attack vector	Attack target	General features
Name	Action 1 …	… Action d ...	… Action n
Terrorist organization	$\beta_{1,j}$ …	… $\beta_{d,j}$ …	… $\beta_{n,j}$

Note: The terrorist behavior profile is calculated by multiplying the weights for each archetype by each individual behavior, and then calculating the sum for each behavior across all archetypes. This method yields a likelihood score for each activity that is between 0 and 1.

how the organization responds to failure since not all actions attempted by terrorists are successful (e.g., a failed bombing or failed recruitment effort). To account for this factor, we propose a rate of adaption to failure (α) to allow for a different speed of learning about an attacking organization when a failed action is observed. This rate could be set for all failures, or it could be tailored to a specific event based on expert assessment and intercepted communication.

Analytically it should be noted that if a terrorist organization was given an α weight of 0 ($\alpha = 0$) by the stakeholders, then an unsuccessful action provides the same amount of information about future behavior as a successful action. In such a case, the updating procedure would be no different, independent of the value of x. If $0 < \alpha < 1$, it would indicate that an observed action still provides some indication of future behavior, but the larger the α value, the smaller the amount of information that can be learned from a failed action.

The second control variable (x) allows stakeholders to control the rate of change for particular terrorist organizations that might be more, or less, prone to change their objectives and tactics. To effectively utilize the model's updating capability, it is important to have $x > 0$. The x value associated with a terrorist organization can be tailored to the specific situation and culture, and could be increased or decreased if there was a change in leadership. One analytic result that is important to note is how changes in α and x impact the rate of change in the weight vector $\boldsymbol{\lambda}_j$. The next section of the paper explores an example application to provide further motivation and context for the proposed method. The following section provides additional insight into the significance of α and x using sensitivity analysis.

For the basic method we have intentionally not included a mechanism to slow the rate of updating over time. Though it would be easy to augment Equation 5 to reduce the step size over time (e.g., $1/j$ or $1/\log(j+1)$), this addition may not be helpful in practice. The utility of this extension would vary widely depending on the application and it could increase the stability of the results. Unfortunately, the increase in stability would also reduce the flexibility of the model by making early actions more important than later actions. Over time, the reduction in step size would result in a reduced space for analysis, and the proposed method could be replaced with other MODA methods where the goal is to find a single decision point (Zionts and Wallenius, 1976, 1983), instead of tracking a dynamic set of preferences and goals.

EXAMPLE APPLICATION

In this section, we explore an example application of archetypes from development to updating. For an example application of archetypes, here we present two possible objectives that a terrorist organization might have: 1. Turn Egypt into an Islamic country, and 2. End US intervention in the Middle East. These two objectives will be used as our example archetypes, and will encompass the entire set of possible objectives for a terrorist organization. For the purposes of this paper we leave the nuances of the elicitation process to the decision maker. Using one of the stakeholder elicitation techniques discussed in the literature review, the characteristics of each terrorist archetype (or decision alternative) would be populated. In our method, the measure of a characteristic is the likelihood of that behavior being exhibited by a terrorist organization with a single objective (one of the archetype objectives).

Once the archetypes have been developed, we can apply the proposed method to try and characterize the behavior of a terrorist organization. In Table 4 we analyze the objectives of a new terrorist organization named SIGMA to provide a starting profile. Since little may be known about this new organization, let the initial archetype vector estimate for SIGMA be equal parts of all known archetypes (initial archetype vector of $\boldsymbol{\lambda}_j = \boldsymbol{\lambda}_0 = (0.5, 0.5)$). Let us assume that SIGMA appears to be a large organization and will be slow to make changes to the organizational objective set ($x = 0.25$). Additionally, let us assume that a failed action provides less information about the objectives of the organization than a successful action ($\alpha = 0.5$).

Although an archetype-based profile could account for a larger number of behaviors, here we focus on a few potential attack vectors that a terrorist organization might pursue: car bomb,

Table 4. SIGMA archetype weight vector.

Terrorist Archetypes (k)	SIGMA weights (λ_0)	Car bomb (d=1)	Suicide bomb (d=2)	Improvised nuclear device (d=3)	Biological attack (d=4)
1. Turn Egypt into an Islamic country	0.5	0.75	0.75	0.05	0.2
2. End American intervention in the Middle East	0.5	0.1	0.5	0.1	0.5

Note: The two terrorist archetypes shown are equally weighted in SIMGA's archetype weight vector. Each value $r_{k,d}$ is the likelihood of a particular type of attack d by archetype k.

suicide bomb, improvised nuclear device, and biological attack. We give each archetype a likelihood of pursuing two attack vectors (actions). Having two potential actions per archetype demonstrates some of the predictive capabilities of the proposed approach, though a simpler example could be constructed with only one potential action.

As shown in Table 5, a single terrorist behavior profile can be generated for a terrorist organization before the attacker has acted based on expert assessment for the types of actions that an organization might exhibit. In this case, our initial archetype weights of $\boldsymbol{\lambda_0} = (0.5, 0.5)$ gives an equal likelihood of the terrorist organization pursuing two different objectives (being composed of two archetypes). In Equation 6, the likelihood of the terrorist organization displaying an action of type d ($\beta_{d,j}$) is calculated using Equation 1. Specifically, Equation 6 shows how to calculate the likelihood that SIGMA would attempt to use a car bomb ($d = 1$) to achieve the organization's objectives. The calculation shown in Equation 6 is repeated for all possible actions ($d \in D$), and the results for this example are shown in Table 5.

$$\beta_{1,0} = \sum_{k=1}^{t} \lambda_{k,j} r_{k,d} = \lambda_{1,0} r_{1,1} + \lambda_{2,0} r_{2,1} = 0.5^{*}0.75 + 0.5^{*}0.1 = 0.425 \quad (6)$$

For this example, the only actions that we have listed are four attack vectors. Now that the list of possible behaviors is identified and associated with an estimate of likely behaviors, we wait until SIGMA acts to update the terrorist profile. Let us assume that the first attack ($j = 1$) by SIGMA was an unsuccessful ($s_1 = 0$) car bomb ($d = 1$), giving us $u_{1,1} = 1$. We know from Table 5 that only terrorists trying to achieve objective 2 would use car bombs, so we can update our terrorist archetype weights using Equation 5 as shown in Equation 7 and solved in Equation 8. Because the attack was unsuccessful, $s_1 = 0$, and a similar calculation is done for the $\boldsymbol{\lambda_{k,1}}$ vector to get all architype weights.

$$\lambda_{k,j} = \lambda_{1,1} = \lambda_{1,0} + x(1 - \alpha(1 - s_1)) \times \left(\frac{r_{1,1}\lambda_{1,0}}{\sum_{k=1}^{t} r_{k,1}\lambda_{k,0}} - \lambda_{1,0} \right) \forall\, k \in [1,t] \quad (7)$$

$$= 0.5 + 0.25 * (1 - 0.5 * 1) \times \left(\frac{0.75*0.5}{0.75*0.5 + 0.1*0.5} - 0.5 \right) = 0.55 \quad (8)$$

After each iteration of the game, a new set of archetype weights ($\lambda_{1,j}, \lambda_{2,j}, \ldots, \lambda_{t,j}$) are calculated for SGIMA's profile. In Table 6, the transformation of each component of the archetype weight vector is updated using the

Table 5. SIGMA behavior profile.

SIGMA Behavior Profile	Car bomb (d=1)	Suicide bomb (d=2)	Improvised nuclear device (d=3)	Biological attack (d=4)
$j = 0$	0.425	0.625	0.075	0.350

Note: The behavior profile for SIGMA ($\boldsymbol{\beta_j}$) is composed of individual estimates ($\boldsymbol{\beta_{d,j}}$), which is the likelihood that SIGMA will attempt action d in an effort to achieve their objectives after the jth action.

Table 6. SIGMA archetype weights over time.

SIGMA archetypes weights after the jth behavior	$\lambda_{1,j}$	$\lambda_{2,j}$
$j = 0$	0.5	0.5
$j = 1$, $s_1 = 0$, $u_{1,1} = 1$	0.55	0.45
$j = 2$, $s_2 = 0$, $u_{2,2} = 1$	0.64	0.36
$j = 3$, $s_3 = 0$, $u_{3,1} = 1$	0.65	0.35

Note: The weight of each archetype changes as new attacks occur, giving a new value for each $\lambda_{k,j}$. This profile can then be used to estimate future attacks.

process shown in Equations 7 and 8 as new events occur. In this example, the events (indexed by j) are: 1. Unsuccessful ($s_1 = 0$) car bomb ($u_{1,1} = 1$), 2. Unsuccessful ($s_2 = 0$) suicide bomb ($u_{2,2} = 1$), and 3. Unsuccessful ($s_3 = 0$) car bomb ($u_{3,1} = 1$).

Each time the SIGMA acts, information can be gleaned about the archetype composition that best represents the motivations and potential future behavior of the organization. Table 6 shows the impact that each new attack has on SIGMA's archetype composition. This gives some insight about the possible motivations of the terrorist organization, and information about potential future attacks as shown in Table 7.

As can be seen in Table 7, after the first car bomb ($u_{1,1} = 1$), a suicide bomb (0.66) or car bomb (0.52) were the most likely future actions, even though SIGMA had only used a car bomb. Since the probabilities were based on archetypes rather than just historical behavior, the probability of other types of events also change as SIGMA's profile changes. This proved insightful in this example because the suicide bomb was expected, and could be thwarted, even though the group had never used this attack vector before.

We can now infer something about one of the key objectives of SIGMA based on the archetype weighting: SIGMA appears to be primarily focused on objective 1, or "Turning Egypt into an Islamic Country," since the weight of Archetype 1 is 0.65. This knowledge can help improve defensive and diplomatic policy, since we can identify some of the goals and methods of the group based on past behavior. However, it is important to note that in the example shown SIGMA still has some portion of their behavior that could be explained based on a secondary objective (Archetype 2). The point of using archetypes is to identify the *set* of objectives that a terrorist organization is attempting to achieve, not just isolate the most likely single objective. This is an especially important point to consider when applying the methodology proposed in this paper.

DISCUSSION

In the previous section, we provided a worked out example of how to assess a terrorist organization (SIGMA), and showed how to use observed actions to gain an initial estimate of an attacker's objectives. The benefit of the archetype method is that after each action, a new profile is developed for the attacker, which provides an estimate of likely future events. Each action provides information about the current state of the attacking organization, and what it may do in the future. As more and more actions are observed (j increases), it is possible that the terrorist organization may have a set of characteristics that are only consistent with one archetype. A result of this type would indicate that the terrorist organization has a clear, singular objective that it is attempting to achieve. This

Table 7. SIGMA behavior profile.

Terrorist profile	Car bomb (d=1)	Suicide bomb (d=2)	Improvised nuclear device (d=3)	Biological attack (d=4)
$j = 0$	0.42	0.62	0.08	0.35
$j = 1$	0.46	0.64	0.07	0.34
$j = 2$	0.51	0.66	0.07	0.31
$j = 3$	0.52	0.66	0.07	0.31

Note: These characteristic compositions are based on the current profile of the SIGMA, and the most recent action, j, and make up the behavior vector $\boldsymbol{\beta}_j$.

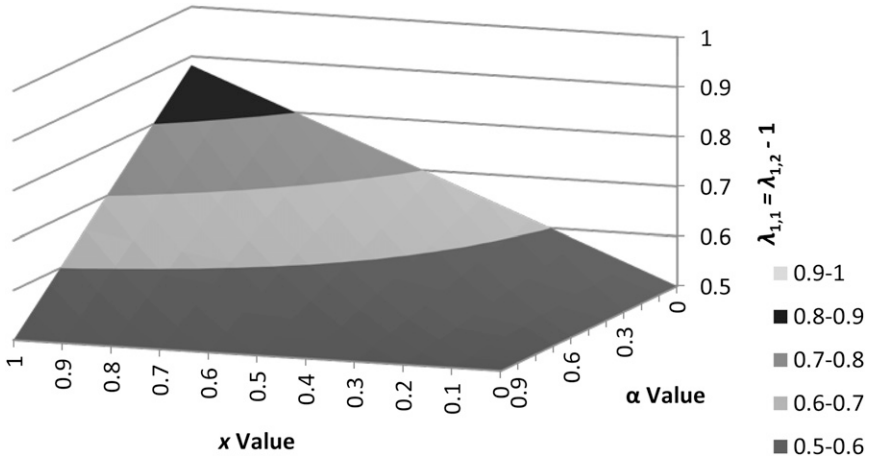

Figure 1. Impact of parameter values. Here we show the new archetype weights for SIGMA after the first action is observed for different parameter values. As x increases and α decreases, the greater the impact of the observed action on the archetype weight λ_j. The black dot indicates the value that was found in this example given the initial parameters for SIGMA.

is one possible outcome of the archetype method, but it is not the only valid result.

As stated in the beginning of the paper, we assume that terrorists do not act randomly. We assume that terrorists are attempting to achieve one or more objectives, and that the actions they attempt will be consistent (in their minds) with achieving those objectives. For this reason, it is important to note that the speed of change in the weighting vector ($\boldsymbol{\lambda}_j$) is highly dependent on the values of α and x. For SIGMA, we set $\alpha = 0.5$ and $x = 0.25$ and only shifted the archetype weight from $\lambda_{1,0}$ to $\lambda_{1,3}$ by 0.15 after observing three actions. In Figure 1 we look at how the result for $\boldsymbol{\lambda_1}$ (the archetype weighting vector after the first action, shown in Table 7) would have been different if SIGMA had a different set of control parameters.

Another analytical result with is important to note is the maximum speed with which an organization might converge on a single archetype. This speed would also be governed by the parameters x and α. In Figure 2 we provide a visual representation of the upper bound for

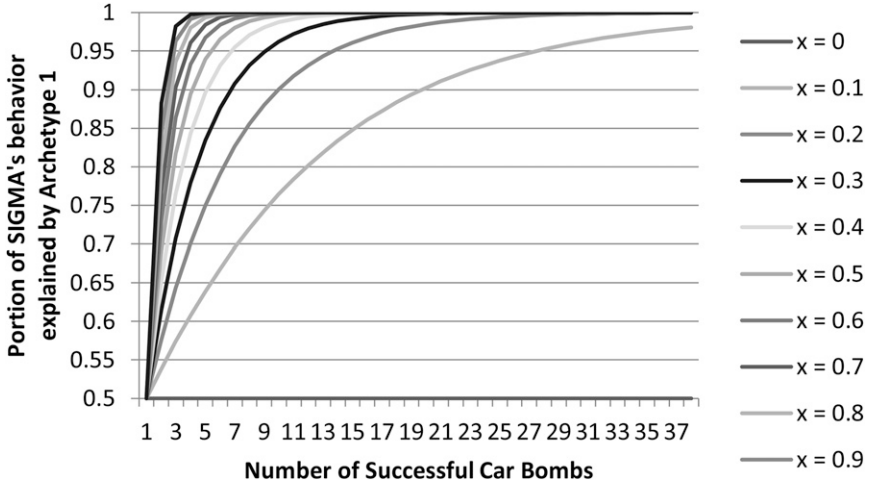

Figure 2. Archetype weighting over time. As the number of observed actions increases, in the unlikely case that all actions are consistent with a single archetype, the weight of that archetype will increase over time.

SIGMA to converge on one archetype, where we assume that SIGMA repeatedly attempted car bombings ($d = 1$). The upper bound would occur if the following conditions were met:

1. The attacking organizations acts in such a way that only one archetype is the most likely to describe the motivation behind every terrorist action.
2. The attacking organization successfully accomplishes every attempted action (of the actions observed) or treats success as being identical to failure ($\alpha = 0$).

In this paper, we attempted to reduce the need for estimation by separating the development of archetypes from the generation of a complicated attacker profile, but there is still a human component that must be considered. The use of expert assessment can tricky and complicated to achieve without introducing bias into a decision (Kynn, 2008). Probability estimation is challenging, and it is important to deal with the issue of bias whenever people's opinions or perspective are involved in a model. In this paper, we have focused primarily on demonstrating the potential value of introducing archetypes and relied on the MODA elicitation literature for a more complete discussion of expert assessment bias (Ford and Sterman, 1998) and implementation in the counterterrorism domain (Bhashyam and Montibeller, 2016).

In future work we plan to explore the impact of allowing an attack, and the impact that such an action would have on the future objectives and actions taken by a terrorist organization. Specifically, if a terrorist organization's objectives can be linked to the actions that are performed, and terrorists respond differently to failure than success, then the defending organization could choose to allow certain actions in order to reduce the chances of more dangerous behavior in the future. For the example, if an organization attempted several peaceful actions (e.g., sit-ins, protests, petitions) but were thwarted when attempting these actions, it's possible that the same organization might attempt more violent actions. If the violent actions are successful, then it's possible that an organization might shift from having peaceful to violent objectives over time. Alternatively, if a previously violent organization attempts to use nonviolent means, how actively should defending governments thwart the nonviolent actions of such an organization?

CONCLUSION

This paper deals with the problem of understanding and adapting to terrorist threats in a practical and statistically viable way. We discuss a new method of profile development for organizations using archetypes, where knowledge about an attacker's objectives and actions can be leveraged to estimate the likelihood of future behavior. In traditional MODA models the objective is to find the decision alternative that best matches the interest of the stakeholders, a method which works well with static preferences and objectives. The contribution of archetypes provides an easy method to develop and update a unique terrorist profile without being constrained by a static modeling structure.

The method proposed in this paper provides a new tool that may improve the ability of government actors to make decisions when faced with an unknown or changing attacker. A model with these capabilities could also help improve decision-making methods over time, even for very complicated attacker profiles. Additionally, the use of archetypes to assess and categorize terrorist organizations could improve efficiency and accuracy when assessing future threats. Rather than building a unique profile of motivations and objectives for each new terrorist organization, agencies will be able to use archetypes to quickly build a terrorist profile. The proposed method could reduce the burden on intelligence and security agencies by allowing them to define the nuanced behavior of terrorist organizations as a combination of general patterns.

ACKNOWLEDGEMENTS

This research was partially supported by the US Department of Homeland Security (DHS) through the National Center for Risk and Economic Analysis of Terrorism Events (CREATE) under award number 2010-ST-061-RE0001. This research was also partially supported by the US National Science

Foundation under award numbers 1200899, 1261058, and 1334930. However, any opinions, findings, and conclusions or recommendations in this document are those of the authors and do not necessarily reflect views of the DHS, CREATE, or NSF. We thank the editors and anonymous referees for their helpful comments. The authors assume responsibility for any errors.

REFERENCES

Alexander, Y., and Swetnam, M. 2001. *Usama bin Laden's al-Qaida: Profile of a Terrorist Network.* Transnational Publishers.

Arango, T., Barnard, A., and Saad, H. 2012. "Syrian Rebels Tied to Al Qaeda Play Key Role in War," *New York Times*, December 8; www.nytimes.com/2012/12/09/world/middleeast/syrian-rebels-tied-to-al-qaeda-play-key-role-in-war.html, retrieved October 31, 2016.

Argomaniz, J. 2013. The European Union Policies on the Protection of Infrastructure from Terrorist Attacks: A Critical Assessment, *Intelligence and National Security,* Vol 30, Nos 1–2, 259–280.

Belton, V., and Stewart, T. J. 2002. *Multiple Criteria Decision Analysis: An Integrated Approach.* Kluwer Academic Publishers.

Bhashyam, S., and Montibeller, G. 2016. In the Opponent's Shoes: Increasing the Behavioral Validity of Attackers' Judgments in Counterterrorism Models, *Risk Analysis,* Vol 36, No 4, 666–680.

Bottomley, P., and Doyle, J. 2001. A Comparison of Three Weight Elicitation Methods: Good, Better, and Best, *Omega*, Vol 29, No 6, 553–560.

Brown, G. G., and Cox, L. A. 2011. How Probability Risk Assessment Can Mislead Terrorism Risk Analysis, *Risk Analysis*, Vol 31, No 2, 196–204.

Cardoso, J., and Diniz, P. 2009. Why Both Game Theory and Reliability Theory Are Important in Defending Infrastructure Against Intelligent Attacks, *Game Theoretic Risk Analysis of Security Threats, International Series in Operations Research & Management Science,* Vol 128, Bier, V., Azaiez, M., Hillier, F., and Price, C., eds., Springer, 1–11.

Chen, L., and Pu, P. 2004. *Survey of Preference Elicitation Methods.* Technical report IC/200467. Swiss Federal Institute of Technology in Lausanne.

Cohon, J. 2004. *Multiobjective Programming and Planning.* Dover Publications.

Cox, L. A. 2008. Some Limitations of "Risk = Threat x Vulnerability x Consequence" for Risk Analysis of Terrorist Attacks, *Risk Analysis*, Vol 28, No 6, 1749–1761.

Crenshaw, M. 2000. The Psychology of Terrorism: An Agenda for the 21st Century, *Political Psychology,* Vol 21, No 2, 405–420.

Cronin, A. 2006. How al-Qaida Ends: The Decline and Demise of Terrorist Groups, *International Security,* Vol 31, No 1, 7–48.

Dalton, A., Brothers, A., Walsh, S., and Paul, W. 2010. Expert Elicitation Method Selection Process and Method Comparison. *Neuroscience and the Economics of Decision Making*, Innocenti, A., and Sirigu, A., eds., University of Siena, Labsi Experimental Economics Laboratory, 182–194.

Ezell, B., Behr, J., and Collins, A. 2012. Identifying Factors that Influence Terrorist Decisions and Target Selection, *Journal of Homeland Security and Emergency Management*, Vol 9, No 1, 1−5.

Ezell, B., Bennett, S., von Winterfeldt, D., Sokolowski, J., and Collins, A. 2010. Probabilistic Risk Analysis and Terrorism Risk. *Risk Analysis*, Vol 30, No 4, 575–589.

Faria, J. 2012. A Vintage Model of Terrorist Organizations, *The Journal of Conflict Resolution*, Vol 56, No 4, 629−650.

Ford, D., and Sterman, J. 1998. Expert Knowledge Elicitation to Improve Formal and Mental Models, *System Dynamics Review,* Vol 14, No 4, 309–340.

Golany, B., Kaplan, E., Marmur, A., and Rothblum, U. 2009. Nature Plays with Dice—Terrorists do Not: Allocating Resources to Counter Strategic vs. Probabilistic Risk, *European Journal of Operations Research*, Vol 192, No 1, 198–208.

Gregory, R., and Keeney, R. 1994. Creating Policy Alternatives Using Stakeholder Values, *Management Science*, Vol. 40, No 8, 1035–1048.

Guikema, S. D., and Aven, T. 2010. Assessing Risk from Intelligent Attacks: A Perspective on Approaches, *Reliability*

Engineering and System Safety, Vol 95, No 5, 478–483.

Guiora, A. 2012. Target Killing: When Proportionality Gets All out of Proportion, *Case Western Reserve Journal of International Law*, Vol 45, Nos 1&2, 235–257.

Insua, I., Rios, J., and Banks, D. 2009. Adversarial Risk Analysis, *Journal of the American Statistical Association*, Vol 104, No 486, 841–854.

Jackson, B., Baker, J., Cragin, K., Parachini, J., Trujillo, H., and Chalk, P. 2005. *Aptitude for Destruction, Volume 2: Case Studies of Organizational Learning in Five Terrorist Groups.* Rand Corporation.

Johnson, T. 2013. Taliban Adaptations and Innovations, *Small Wars & Insurgencies*, Vol 24, No 1, 3–27.

Keeney, R. L. 2007. Modeling Values for Anti-Terrorism Analysis, *Risk Analysis*, Vol 27, No 3, 585–596.

Keeney, R., and von Winterfeldt, D. 1989. On the Uses of Expert Judgment on Complex Technical Problems, *IEEE Transactions on Engineering Management*, Vol 36, No 2, 83–86.

Kynn, M. 2008. The ''Heuristics and Biases'' Bias in Expert Elicitation, *Journal of the Royal Statistical Society: Series A (Statistics in Society)*, Vol 171, No 1, 239–264.

Linkov, I., Wenning, R., and Kiker, G. A. 2007. *Managing Critical Infrastructure Risks.* Springer.

Medina, R. 2014. Social Network Analysis: A Case Study of the Islamist Terrorist Network, *Security Journal*, Vol 27, No 1, 97–121.

Mishal, S., and Rosenthal, M. 2005. Al Qaeda as a Dune Organization: Toward a Typology of Islamic Terrorist Organizations, *Studies in Conflict and Terrorism*, Vol 28, No 4, 275–293.

Pate-Cornell, E., and Guikema, S. 2002. Probabilistic Modeling of Terrorist Threats: A Systems Analysis Approach to Setting Priorities Among Countermeasures, *Military Operations Research*, Vol 7, No 4, 5–20.

Post, J. 1984. Notes on a Psychodynamic Theory of Terrorist Behavior, *Terrorism*, Vol 7, No 2, 241–256.

Post, J. 1986. Hostilité, Conformité, Fraternité: The Group Dynamics of Terrorist Behavior, *International Journal of Group Psychotherapy*, Vol 36, No 2, 211–224.

Post, J., Ruby, K., and Shaw, E. 2002. The Radical Group in Context: 2. Identification of Critical Elements in the Analysis of Risk for Terrorism by Radical Group Type, *Studies in Conflict & Terrorism*, Vol 25, No 2, 101–126.

Riabacke, M., Danielson, M., Ekenberg, L., and Larsson, A. 2009. A Prescriptive Approach for Eliciting Imprecise Weight Statements in an MCDA Process, *Algorithmic Decision Theory*, Lecture Notes in Computer Science, Vol 5738. Springer, 168–179.

Ribeiro, R. 1996. Fuzzy Multiple Attribute Decision Making: A Review and New Preference Elicitation Techniques, *Fuzzy Sets and Systems*, Vol 78, No 2, 155–181.

Rostow, N. 2002. Before and After: The Changed UN Response to Terrorism Since September 11th, *Cornell International Law Journal*, Vol 35, Winter, 475–490.

Russell, C., and Miller, B. 1977. Profile of a Terrorist, *Studies in Conflict and Terrorism*, Vol 1, No 1, 17−34.

Satha-Anand, C., and Urbain, O. 2013. *Sacred Spaces and Accursed Conflicts: A Global Trend? Protecting the Sacred, Creating Peace in Asia Pacific, Peace and Policy*, Vol 17, Transaction Publishers, 7–52.

Triantaphyllou, E., and Baig, K. 2005. The Impact of Aggregating Benefit and Cost Criteria in Four MCDA Methods, *IEEE Transactions on Engineering Management*, Vol 52, No 2, 213–226.

Trindal, J. 2013. *Gas Refinery Attack in Algeria: The Lessons Learned.* Domestic Preparedness (March 20) www.domesticpreparedness.com/resilience/gas-refinery-attack-in-algeria-the-lessons-learned, retreived October 31, 2016.

Victoroff, J. 2005. The Mind of the Terrorist: A Review and Critique of Psychological Approaches, *The Journal of Conflict Resolution*, Vol 49, No 1, 3–42.

Wallenius, J., Dyer, J., Fishburn, P., Steuer, R., Zionts, S., and Deb, K. 2008. Multiple Criteria Decision Making, Multiattribute Utility Theory: Recent Accomplishments and What Lies Ahead, *Management Science*, Vol 54, No 7, 1336–1349.

Walzer, M. 2013. Code: Can the Good Guys Win, *European Journal of International Law*, Vol 24, No 1, 433–444.

Wang, C., and Bier, V. 2011. Target-Hardening Decisions Based on Uncertain Multiattribute Terrorist Utility, *Decision Analysis*, Vol 8, No 4, 286–302.

Willis, H., and Kelly, T. 2005. *Estimating Terrorism Risk.* RAND Corporation.

Yu, P., Lee, Y., and Stam, A. 1985. *Multiple-Criteria Decision Making: Concepts, Techniques, and Extensions.* Plenum Press.

Zionts, S., and Wallenius, J. 1976. An Interactive Programming Method for Solving the Multiple Criteria Problem, *Management Science*, Vol 22, No 6, 652–663.

Zionts, S., and Wallenius, J. 1983. An Interactive Multiple Objective Linear Programming Method for a Class of Underlying Nonlinear Utility Functions, *Management Science*, Vol 29, No 5, 519–529.