ASSESSING THREAT SCENARIOS: SEVERITY, MITIGATION, CAPABILITY AND RESPONSE

Ami Arbel
Industrial Engineering
Tel Aviv University
Tel Aviv 69978, Israel

Amos Guiora
S.J. Quinney College of Law
University of Utah
Salt Lake City, UT 84112, USA

Luis G. Vargas*
The Joseph M. Katz Graduate School of Business
University of Pittsburgh
Pittsburgh, PA, 15260, USA
E-mail: lgvargas@pitt.edu

ABSTRACT

Terrorism is generally viewed as: "the use of violence and intimidation in the pursuit of social, political, economic or religious aims." Today's corporations face increasing threats from foreign and domestic groups. These threats can be exerted both physically and financially, both in real space as well in cyber space. Threats can be generated both by terror groups as well as those operating merely for personal financial gains. In this paper we provide a novel methodology for dealing with threats, assessing their scope, mitigating their impact, and generating proper feasible responses. This phase is followed by screening those generated options into a set of responses in line with current capabilities and time constraints.

Keywords: Threat assessment, scenario evaluation, terrorism

1. Introduction

Terrorism is generally viewed as: "the use of violence and intimidation in the pursuit of social, political, economic or religious aims." More generally, in a recent book Amos Guiora (Guiora 2008) defines terrorism as: "… the killing, injuring, or intimidation of, or causing property damage to, innocent civilians by an individual or group seeking to advance a social, political, economic, or religious cause." Today's organizations face increasing threats from foreign and domestic groups. These threats can be exerted both physically and financially, both in real space as well in cyber space. Threats can be generated both by terror groups as well as those operating merely for personal financial gains. In this paper we develop a process enabling us to see the big picture emanating from such threats to organizations livelihood and longevity. Specifically, we address the following issues:

- What are threats?
- How do you map out potential feasible threat scenarios?
- How do you assess their potential damage?
- How do you respond to a threat?
- How do you determine cost-benefits of responses?

* Corresponding author

- How do you create a secure environment for an organization's assets, employees and customers both domestically and globally?

All of these lead to the main question: *"How do you prepare an organization for a terrorist/threat attack by developing and implementing preventive measures intended to mitigate those threats?"*

2. Background

This paper deals with a broad problem involving multitude of issues whose proper timely and purposeful treatment is of high value. While the basic premises of the problem seem to be self-evident in their importance and immediate need, surprisingly, very little has been done to formally address this problem in its broadest scope and provide a workable framework of implementable analysis. The US Department of Homeland Security has realized a need for developing a framework of analysis capable of identifying potential threats, assess the capabilities of adversaries, mitigate their actions and select the best course of action in response to the threats. Surprisingly enough, such a system does not exist in today's operational world. A recent report (Schanzer and Eyerman 2009) characterizes strategic risk management as a highly complex exercise, fraught with difficulties. Specifically, according to that report "… while significant progress has been made at DHS theoretical, structural, and political obstacles currently frustrate its ability to allocate its resources based on risk management principles: Analytic tools have not been fully developed to deal with the risks created by adaptive adversaries or to compare risks across different threat areas …" Clearly then, the need for such a framework exists and has been recognized.

Some approaches have been developed in the past; however, none is fully capable of addressing the formidable scope of the problem of assessing and responding to terrorist threats. Looking at such approaches, the first one the comes to mind - and one of the earliest methodologies developed for general decision making problems - is the one termed *Decision analysis Under Uncertainty*. This is a systematic application of probability and utility theory to problems of choice among alternatives in risky environments (Luce and Raiffa 1957). As such, it has developed over the last decades into a mature and powerful approach capable of handling a large number of problems, and there are many well-developed techniques for assisting the decision maker in choosing among competing alternatives. It should be noted, however, that this is the approach taken by the *rational choice theory* school (Paté-Cornell and Guikema 2002) There are researchers who do not advocate the use of the rational choice school decision analysis (Green and Shapiro 1996). In practice, however, a decision analyst merely aids the decision maker in specifying the alternatives (options generation) as well as in assessing the value of these alternatives (choice resolution). It is somewhat puzzling, then, to find that "Practiced decision analysts... report that a major part of many studies is the specification of the set of alternative courses of action" (Watson and Brown 1978).

This observation has raised the specific question of how do these courses of action are actually generated. This has led to an extension of the existing theory that is best classified as *Option Generation in Decision Problems* (Arbel and Tong 1982; Keller and Ho 1988). A search of the decision sciences literature indicates an almost complete lack of interest in problem specification. It has been suggested that the reason for this is that decision scientists view options generation as an act of *creative insight* and thus not addressable by normative techniques. Such an attitude would seem somewhat shortsighted. The psychology literature is replete with studies which show that, even in the most favorable circumstances, human decision makers exhibit suboptimal behavior and are prone to focus on a narrow range of alternatives. A prominent example of such behavior was identified by H.A. Simon (Simon 1972) who explored what he termed the "bounded rationality" of decision making. In the context of that work, he termed the actual behavior of Decision Makers (DM) as that of a 'satisficing' approach to decision making. That is, a 'good-enough' choice making, rather than searching for the best. A practical theory should address all aspects of the problem, not just those which are mathematically tractable and quantifiable.

A somewhat different class of methods of dealing with the problem involves enumerating all relevant issues affecting outcomes. Such a tool is termed a ***scenario generation*** approach. This involves forecasting outcomes of possible events that form specific scenarios. Unfortunately, such an approach is usually a quite difficult even when all the details of scenarios are known due to the high dimensionality of all possible outcomes. To make things even worse, deciding what scenarios are relevant and more likely to occur is far from being a trivial task. A special case of this class of approaches is offered by the so-called *Morphological Analysis* (MA)(Ritchey 2004). MA exhaustively maps out all dimensions of identified potential threats. This approach helps to systematically identify parameters of threat scenarios, levels of threats within each parameter and possible inconsistencies between parameter values of different threats. Each of the identified threat scenarios produces consequences along different dimensions such as social (e.g., injuries, fatalities, psychological damage), financial (e.g., loss of stock value, loss of assets), economic (e.g., plant destruction, supply disruption), corporate (e.g., image) and so on. These consequences require very specific courses of action to mitigate the threat and respond appropriately to minimize the consequences. It should be pointed out, however, that such an exhaustive generation of threat scenarios does not contribute to clarify the problem but, rather, tend to obscure the choice needed to address the issues/threats. In addition, the scenarios, by their very nature, are descriptive rather than prescriptive. That is, they do not help to make choices as far as actions and responses to threats.

What people do now is they assume a future represented by a scenario. The risk of the scenario is measured by the probability of its occurrence (threat) times the probability that there is damage given the attack (vulnerability) times the expected damage from the attack given that it happened and resulted in some damage (Willis et al. 2005) i.e.,

Risk = P[attack occurs]*P[attack results in damage|attack occurs]*E[damage|attack occurs and results in damage] =
Threat * Vulnerability * Consequence.

Thus, to assess the risk of a scenario we need to know the likelihood of its occurrence and the damage. Current methods start with the premise that a scenario is given and proceed to analyze it. The question is: How do we get to the given scenario? The main problem is: How to envision the future scenarios and identify the dimensions of concern.

(Jackson and Frelinger 2009) suggest a scheme to decide which targets are more amenable to a threat, but they do not believe that a rigorous evaluation is possible. (Lempert et al. 2003) have studied four basic approaches to address long term policy analyses: (1) Group narrative processes, e.g., Delphi method, foresight exercises; (2) Simulation modeling; (3) Decision Analysis; and (4) Scenario development. They point out that these approaches have weaknesses that make them questionable to be used for long term policy analyses. This is not the only author who thinks that we need new methodological developments to address the problems involved in risk assessment. (Schanzer and Eyerman 2009) write:

"Analytic tools have not been fully developed to deal with the risks created by adaptive adversaries or to compare risks across different threat areas….Risk tradeoffs are often political decisions that require public input, but mature methodologies for receiving such input have not been developed."

In this paper we propose the use of the Analytic Network Process (ANP) (Saaty 2001). The ANP has its foundations on the Analytic Hierarchy Process. The AHP is grounded on the judgments of experts. The judgments used are absolute and are used to measure the relative influence of intangible and tangible factors in decision making. The strength of this theory is in group decision making. Because cardinal judgments do not violate Arrow's conditions (Saaty and Vargas 2011), it is possible for a group to arrive at decisions satisficing the criteria of decision makers.

3. Proposed Approach

Before proceeding with our proposed approach it should be emphasized that the core element deals with scenario threat dimension. This, however, is clearly a highly sensitive subject that is not expected to be

discussed openly. Therefore, our approach uses a generic threat dimension devoid, perhaps, of connection to any real case.

An important basic distinction between other methodologies (e.g., (Paté-Cornell and Guikema 2002) and ours is that we are interested in finding out what is important to address a threat not how likely it is. Thus, we are interested in finding the best way to respond to a threat. In the process of ascertaining how important a threat is we will also assess some relative likelihood of occurrence, but this is not the primary objective of the methodology.

As an example of how to characterize a threat and how it can be represented, we identified dimensions or attributes that eventually will determine its likelihood (See Table 1). According to (Schanzer and Eyerman 2009) threats are defined by their (a) operational complexity and difficulty and (b) the potential operational breakdowns. We consider these dimensions but add other factors that are crucial to determining the reality of the threat such as the quality of the intelligence available and uncontrollable factors.

Table 1. Threat Characteristics

Operational Complexity and Difficulty	**Uncontrollable Factors (unknowns)**
Technology	Who?
Feasibility	Where?
Level of Sophistication	When?
Skill	How?
Coordination	Population Response
Potential Operational Breakdowns	Additional Attacks Possible?
Prevention	Capabilities Operational?
Detection	Who has Jurisdiction?
Quality of Intel	Type of Danger Posed?
Reliability of Source	Legal Issues?
Viability	Backup Systems Operational?
Relevance (time sensitive)	How do you know it works?
Corroboration	Counter responses to our actions?
	Ripple effect

For a specific threat, these dimensions cannot be prioritized in a vacuum. They need to be considered within a global scheme that considers: (1) consequences, (2) capabilities, (3) constraints, (4) responses and (5) consequences of responses. The relationships and influences among these components are illustrated in Figure 1.

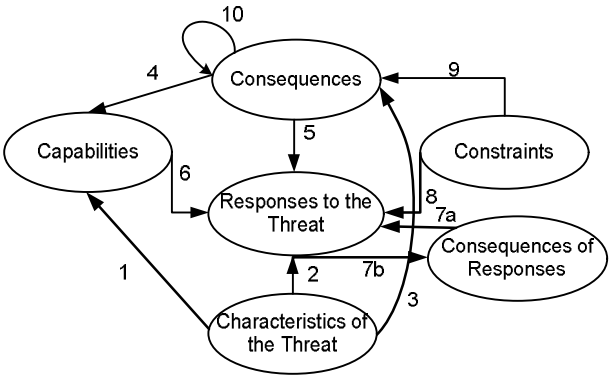

Figure 1. Assessing Threat Scenarios

An arrow from node A to node B represents the influence of node A on node B and in the context of the ANP it is used to ask questions that will lead to prioritization.

1. Given a Threat Characteristic which Capability is best to mitigate/neutralize the threat
2. Given a Threat Characteristic which Response is best to mitigate/neutralize the threat
3. Given a Threat Characteristic which Consequence is more critical
4. Given a Consequence which Capability can help best to mitigate its effects
5. Given a Consequence which Response is better to address the Consequence
6. Give a Capability which Response is best supported by it

7a. Given a Consequence from a Response which Response is more acceptable

7b. Given a Response which Consequence from that Response is more critical

8. Given a Constraint which Response best takes that Constraints into account
9. Given a Constraint which Consequence is more important
10. Given a Consequence (e.g., disruption of operations) which other consequence is more influenced by it.

The goal of this process is to derive the net influence of all the components on "the responses to the threat" to decide which course of action is most appropriate, whether or not existing capabilities are suitable to address the threat, and what type of constraints must be eliminated or overcome to mitigate damages.

Each of the arrows in Figure 1 represents the influence of a node on another. A node is a cluster of elements. Since each node or cluster consists of several elements, sometimes an entire network as in the case of Consequences, we must identify to which elements in other clusters each element in a cluster must be connected. Table 2 shows the suoermatrix that would obtain after the influences are evaluated.

4. Concluding Remarks

There is an urgent need for developing a counter-threat strategy that is integrated into an organization's operating procedures in order to minimize the impact of threats on the potential growth of the organization. The limit supermatrix will yield the response(s) that best takes into account the consequences of the threat, the existing capabilities that will best help mitigate the threat, and the relative evaluation of the threat dimensions from which it should be possible to determine the likelihood of occurrence the threat, not because of the priorities but because the priorities will point out the weaknesses and strengths of the threat.

REFERENCES

Arbel, A. and R. M. Tong (1982). "On the Generation of Alternatives in Decision Analysis Problems." J. of the Operational Research Society **33**(4): 377-387.

Green, D. P. and I. Shapiro (1996). Pathologies of the Rational Choice Theory School, Yale University Press.

Guiora, A. N. (2008). Fundamentals of Counterterrorism. New York, Aspen Publishers.

Jackson, B. A. and D. R. Frelinger (2009). Emerging Threats and Security Planning: How should we decide what hypothetical threats to worry about? Occasional Paper Series, RAND Homeland Security.

Keller, L. R. and J. L. Ho (1988). "Decision Problem Structuring: Generating Options." IEE Transactions on Systems, Man and Cybernetics **18**(5): 715-728.

Lempert, R. J., S. W. Popper and S. C. Bankes (2003). Shaping the next one hundred years: new methods for quantitative, long-term policy analysis, The RAND Pardee Center.

Luce, R. D. and H. Raiffa (1957). Games and Decisions. New York, Dover Publications, Inc.

Paté-Cornell, E. and S. Guikema (2002). "Probabilistic Modeling of Terrorist Threats: A Systems Analysis Approach to Setting Priorities Among Countermeasures." Military Operations Research **7**(4): 5-20.

Ritchey, T. (2004). Developing Threat Scenarios and Strategy Models with Computer Aided Morphological Analysis. Advanced Simulation Technologies Conference, Arlington Virginia, USA.

Saaty, T. L. (2001). The Analytic Network Process: Decision Making with Dependence and Feedback. Pittsburgh, PA, RWS Publications.
Saaty, T. L. and L. G. Vargas (2011). "The Possibility of Group Choice: Pairwise Comparisons and Merging Functions " Social Choice and Welfare (To Appear).
Schanzer, D. H. and J. Eyerman (2009). Improving Strategic Risk Management at the Department of Homeland Security. Strategic Risk Management in Government: A Look at Homeland Security, IBM Center for The Business of Government.
Simon, H. A. (1972). Theories of Bounded Rationality. Decision and Organization. C. B. McGuire and R. Radner, North-Holland Publishing Company**:** 161-176.
Watson, S. R. and R. V. Brown (1978). "Valuation of decision analysis." J.R. Statistical Society Series A **141**(1): 69-78.
Willis, H. H., A. R. Morral, T. K. Kelly and J. J. Medby (2005). Estimating Terrorism Risk, RAND Center for Terrorism Risk Management Policy.

Table 2. The supermatrix