DRAFT

Report #05-006

SURVEY OF LITERATURE ON STRATEGIC DECISION MAKING IN THE PRESENCE OF ADVERSARIES

Kardes, E. & Hall, R.

CREATE REPORT
Under FEMA Grant EMW-2004-GR-0112

March 15 , 2005

Center for Risk and Economic Analysis of Terrorism Events
University of Southern California
Los Angeles, California

3710 McClintock Avenue, RTH 314 Los Angeles, CA 90089-2902 ~ (213) 740-5514 ~ www.usc.edu/create

Survey of Literature on Strategic Decision Making in the Presence of Adversaries

CREATE Interim Report

March 15, 2005

Erim Kardes
Randolph Hall
Epstein Department of Industrial and Systems Engineering
University of Southern California

ABSTRACT

This report reviews methodologies and applications in the literature pertaining to decision making problems in the presence of adversaries. This investigation is essentially motivated by the need to determine optimal strategies against an adversarial and adaptive opponent. Such a problem arises in the context of terrorism threats. Probabilistic risk analysis is an insightful approach to this end; however, it lacks the essential adversarial decision processes perspective. Hence, applications of game theory in this context are examined, followed by its combination with other approaches. Possible future research areas are described subsequently.

ACKNOWLEDGMENT

This research was supported by the United States Department of Homeland Security through the Center for Risk and Economic Analysis of Terrorism Events (CREATE), grant number EMW-2004-GR-0112. However, any opinions, findings, and conclusions or recommendations in this document are those of the authors and do not necessarily reflect views of the U.S. Department of Homeland Security.

Introduction

The threat of catastrophic terrorism has motivated multi-billion dollar investments in the United States and elsewhere, with the goal of improving safety and security. Investments of this magnitude demand careful consideration of the costs of implementation, operation and maintenance, as well as the benefits derived from a reduction in exposure to future losses.

Unlike naturally occurring or accidental events -- such as floods, earthquakes or system failures -- terrorism is fundamentally adversarial. Thus investments designed to protect against one type of terrorism (e.g., against blasts, biological agents, or radiological devices) have potential to elevate the risk of other types of terrorism. Moreover, investments targeted at reducing the general effectiveness of terrorist organizations, or targeted at the willingness of individuals to engage in terrorism, may protect against multiple types of terrorism.

Terrorism is also fundamentally different from the risk of warfare among states, especially when it is not state sponsored. Conventional warfare is a less random occurrence than terrorism because state adversaries are more likely to announce their specific intentions and because their actions are more easily monitored through surveillance. States are also more easily deterred through the threat of a specific military response that inflicts losses on the adversary. In the case of terrorism, the opponent attacks with greater frequency, with greater randomness, and often without the opportunity of deterrence through a direct military response. Thus both the methods of protecting against warfare, and the methods for analyzing the threat, are fundamentally different than they are for terrorism.

Last, terrorism also differs from other intentional criminal acts. As witnessed on 9/11, terrorism has potential to produce more catastrophic events than simple criminal acts, as well as to introduce radically new tactics in its effort to produce fear. Tools used to model exposure to criminal losses, which are common in the insurance industry, are not easily modified to evaluate adaptable terrorist adversaries.

One goal of the Center for Risk and Economic Analysis of Terrorism Events (CREATE) is to develop tools to guide investments in counter terrorism, accounting for economic costs and benefits, and accounting for non-state-based terrorist risk. Toward this end, this paper reviews literature on strategic decision making, drawing from three main fields: probabilistic risk analysis, game theory, and reliability. It is important to note that research efforts are not isolated merely in a single field and combinations of these fields have been of interest in developing new techniques and applications.

The purpose of this report is to present methodologies and applications in the literature pertaining to adversarial decision making problems and to suggest topics for future research addressing terrorist risks that represents decision-making in the presence of noncooperative opponents. Adversarial decision-making could be interpreted as

strategic planning of responses to the actions of attackers, which are not completely observable.

This report is organized as follows. Section 2 introduces important documents related to probabilistic risk analysis. Section 3 presents pure game theoretic approaches to model terrorism/security related problems. Section 4 introduces combinations of methodologies applied or that could be applicable to security modeling. Section 5 introduces stochastic games and a small portion of the related literature. Section 6 presents two other mathematical modeling approaches. Finally, the concluding section suggests topics for future research.

Probabilistic Risk Analysis (PRA)

The PRA method was initially developed for the purpose of assessing the safety of nuclear reactors. Expert elicitation is typically used as an input to risk models along with historical failure data. Bayesian methods are also frequently used in PRA, which is affected by the assumed prior probability distributions (Bernard, 2004). In this section we focus on the application of PRA to adversarial risks.

Hudson et al. (2002) introduced a tool built to assist antiterrorism planners at military installations to draw inferences about the risks of a terrorist attack. This tool allows antiterrorism planners to analyze and manage a large portfolio of risks simultaneously by encoding the knowledge about assets and risks into Bayesian network fragments that could be dynamically combined at run-time into a Bayesian network for assessing risks specific to a given installation and situation. The data sources for this hierarchical network include the planner's own subjective assessments, historical database information, analytical model results and simulation results integrated into various nodes on the Bayesian network. The network is dynamically constructed by the tool and is solved and presented to the user for each combination of asset and threat that the user describes.

Laskey and Levitt (2002) provide a practical, computational methodology to encode a distributed library of patterns for automated reasoning about aspects of homeland defense against terrorism. Multi-Entity Bayesian networks (MEBNs) provide a means of encoding repeated patterns and relationships in the form of network fragments. These fragments are combined to form situation specific Bayesian networks. Authors propose the use of MEBNs as the inferential cornerstone of a cumulative national, distributed knowledge base for homeland defense. This paper illustrates the use of MEBNs with an example concerning a multi-city coordinated bio-warfare attack. Authors attempt to show how current trends in the use of on-line reporting by health care and related facilities have the potential to enable opportunistic detection of and response to such an attack.

Weaver et al. (2001) describe a research effort to develop models of terrorist organizations that will permit to stimulate and predict what types of decisions these organizations and their agents might be likely to make. Authors contend that terrorist

organizations and individual decision makers can be described via Markov Decision Processes and repeated Bayesian networks. Another task of this research is to gather literature sources and to assemble a database that contains profiles of a reasonable sample of terrorist organizations and to use this information in conjunction with the models developed.

Singh et al. (2004) develop a tool to detect and track terrorist activity. Authors follow two probabilistic approaches: Hidden Markov Models (HMMs) and Bayesian networks (BNs). Authors assert that HMMs, which are used for modeling partially observed stochastic processes, are an ideal way to make inferences about the evolution of terrorist networks. The HMMs detect the monitored terrorist activity and measure threat levels, whereas BNs combine the likelihoods from many different HMMs to evaluate the cumulative probability of terrorist activity. In other words, BNs represent the overarching terrorist plot and the HMMs, which are related to each BN node, represent detailed terrorist subplots. A case study for the 2004 Olympics is presented in this paper as an example.

Haimes (2002) offers a holistic risk assessment and management framework for modeling the risks of terrorism to the homeland. According to this paper, two major interconnected systems are the homeland and the terrorist network systems. The variables pertaining to the two systems are considered and their interactions are presented in a schematic way.

Many other articles on PRA related to security modeling, some of which are cited here, are referred to in Bier (2004). Although PRA is helpful to gain insight about security risks, it lacks the decision perspective that is extensively present in the security risk modeling domain. Hence, the next section is devoted to another approach that could confront this adaptive perspective.

Game Theory

Social scientists have written many papers on applications of game theory to terrorism, as explained in Sandler and Arce M. (2003). The authors contend that game theory captures the strategic interactions among terrorists and targeted governments, that is between players, where actions are interdependent and neither of the sides can be considered passive. Other reasons include the rationality assumption of the players in games and ability of games to represent gains or losses to a player through payoffs. The main purpose of this paper is to review how game theory has been used in the literature and to present new applications that include terrorists' choice of targets, governments' choice between preemption and deterrence, and the government concessionary policy when terrorists are of two minds: hard-liners and moderates. For example, for the choice between preemption and deterrence, a three-player game is played in normal form that includes the US, the UK and the terrorist organization. For the government concessionary problem, a model of bargaining between a government and a terrorist group with moderate and hard-line members is considered.

It is important to note that Sandler and Arce (2003) use a simple game theory model to answer high-level, generic questions. The authors note that the model would benefit from a multi-period analysis of terrorist campaigns, where terrorist resource allocation is studied over time. Another area of future work could be differential games to examine how terrorist organizations are influenced by successful and failed operations. The dynamics of strategic choices of both players can be captured with this approach by modeling for the rate of change over time of resources for each player. Finally, the authors note that cooperative game theory has never been applied to the study of terrorism, which would enable analysis of shared intelligence, training facilities, and operatives to strengthen their abilities.

Sandler et al. (1983) present models that depict the negotiation process between terrorists and government policymakers for incidents where hostages are seized and demands are issued. Lapan and Sandler (1988) present a game in extensive form where the government first chooses the level of deterrence that consequently determines the logistical failure or success of terrorists when they engage in a hostage mission. Atkinson et al. (1987) extend Nash's bargaining game, where time is taken into consideration. Sandler and Siqueira (2002) present an application of game theory that involves terrorists' choice of targets for a three-player game involving two targeted governments and a common terrorist threat. Lapan and Sandler (1993) analyze a scenario via a two-period game, where the government is incompletely informed about the terrorists' capability. The extent of terrorist attacks in this scenario can provide information to the government about the type of the terrorist group.

Faria (2003) makes two contributions to the literature on terrorism: 1) It presents a model that explains the cyclical characteristic of terrorist attacks, and 2) It improves on the existing theoretical cyclical models since it takes into account terrorists' motivations and decision-making explicitly. A differential game is used between terrorists and the government in which terrorists maximize the number of attacks subject to a constraint that combines terrorists' resources and government anti-terrorist policies. This model is a standard microeconomic model, where the representative terrorist group solves a maximization problem based on preferences, actions, incentives, and budget restrictions. The government problem concerns the maximization of national security. The solution of the terrorist problem yields a time path for terrorist activities. The government takes the time path of terrorist activities into account when maximizing national security over time. The solution of the government problem yields a limit cycle between enforcement and terrorist activities. The permanent cyclical paths in enforcement and terror cause national security and terrorist stocks to display cyclical trajectories as well.

D'Artigues and Vignolo (2003) study the emergence of the recent form of terrorism using evolutionary game theory. The model in this paper presents terrorism as the result of competition between countries, when the desire to imitate the leading country is frustrated by the impossibility of doing so. Authors define a multi-country setup where interaction takes place in an international trade game, which is a coordination game. In

particular, this paper uses the evolutionary game model to describe the long-run behavior of *n* countries.

Kunreuther and Heal (2003) consider security as a problem among agents and focus on situations where the security levels of members of a group are interdependent. The main idea in this paper is that the dependence of one agent's security on the behavior of others may partially or completely negate the payoffs it receives from its own investment in protective measures. These cross-effects are referred to as *contagion*. Authors illustrate this argument by reference to an airline that attempts to determine whether to install a baggage checking system. In making this decision, the airline needs to balance the cost of installing and operating such a system with the reduction in the risk of an explosion from a piece of luggage not only from the passengers who check in with it, but also from the bags of passengers who check in on other airlines and then transfer to it. In this example, the incentive to invest in security decreases if other airlines fail to adopt protective measures. As the authors indicate, this paper examines the case where all agents are identical. Heal and Kunreuther (2003) consider situations where the agents have different protection costs and risks, and where the actions creating potential losses are impacted by agents' protective decisions. Future research directions suggested in the paper include examining how agents behave in multi-period models and determining appropriate behavioral models of choice that could characterize individuals who make imperfectly rational decisions.

Major (2002) presents another application of game theory, which includes a simplified model of terrorism risk to develop a probability distribution of losses. However, this effort captures only the severity component of risk that is of potential interest to the insurance professionals. The losses that could occur with certain probabilities are revealed given that an attack is attempted.

Application of game theory to security is a suitable way to model adversarial decision-making processes. However, limiting analysis to this approach is still a simplification. Game theory applications could be supported with additional modeling methodologies as described below.

Combination of Game Theory and Other Approaches

Game Theory and Influence Diagrams

Pate-Cornell and Guikema (2002) present a generic influence diagram model for setting priorities among threats and among countermeasures. The random variables used in the authors' first model is fairly generic and account for types of terrorist groups, their access to materials, cash, types of weapons, and etc. For instance, only one decision variable is used to represent U.S. countermeasures. The authors' next model elaborates on the previous one by considering two influence diagrams: one for the terrorist behavior and the other for the U.S. Results pertaining to the influence diagram for terrorist behavior are then used as inputs to the influence diagram for US. Hence, this model is

called “two-sided”. The authors then consider using the two-sided diagram in a dynamic fashion via discrete time steps. At each step, each side updates its beliefs, objectives, and decisions based on the previous step. It is also denoted that each side is uncertain about the other’s actions and state of knowledge. According to the authors, another change that needs to be included in the model is the evolution of the organizations involved, the emergence of new groups, or a new structure of existing groups and networks. Although these ideas are put forward, no implementations or quantitative illustrations exist with regards to the dynamic approach or evolutions of organizations.

According to Koller and Milch (2001), the traditional representations of games using the extensive form or the normal form obscure much of the structure that is present in real-world games. Hence, authors propose a new representation language, named multi-agent influence diagrams (MAID), for general multi-player games. This approach extends influence diagrams to a context where more than one decision maker is involved, an idea first examined by Shachter (1986). MAIDs allow the dependencies among variables to be represented explicitly, whereas both the normal and the extensive form obscure certain important relationships among variables. MAIDs representation extends the Bayesian network formalism (Pearl, 1988) and influence diagrams (Howard and Matheson, 1984) to account for the decision problems involving multiple decision makers. They have defined semantics as non-cooperative games. Just as Bayesian networks make explicit the dependencies among random variables, MAIDs make explicit the dependencies among decision variables. They are also related to the formalism presented by La Mura (2000), where network representation for games is developed. Solutions to MAIDs consider the strategic independence structure on the diagram. Extensions to this research could be establishing the relations among competitive Markov decision processes, stochastic games, and MAIDs. Another extension could be exploring ways to integrate the issue of evolution over time into the MAIDs framework.

Brynielsson and Arnborg (2004) review some military applications of gaming and introduce a game component into an influence diagram example. Authors illustrate the use of Bayesian game-theoretic reasoning for operations planning by transforming a decision problem into a Bayesian game.

Virtanen et al. (2004) describe a multistage influence diagram game for modeling the maneuvering decisions of pilots in one-on-one air combat. Virtanen et al. (2004b) describe an extension of the influence diagram approach into a dynamic multistage setting without any game aspect. Authors contend that this paper is the first elaboration where ideas regarding multi-agent multi-period influence diagrams are combined and implemented. Dynamic programming is considered for the solution of the model in this paper. To cope with the combinatorial explosion, authors trade the solution of the complete game with the computing time and apply a moving horizon control approach, where the horizon of the original influence diagram is truncated and a dynamic game with a shorter planning horizon is solved at each decision instant. Instead of the whole duration of the game, this approach allows the players to update their information about the state of the system at any moment over the limited planning horizon.

Virtanen et al.'s solution approach is inspired by Cruz et al. (2002), who contend that dynamic game theory is a suitable formulation for problems that involve adversaries interacting with each other over a time period. Cruz et al. (2002) denote that traditional solutions from dynamic game theory that involve optimizing objective functions over the entire time horizon of the system are extremely difficult but not impossible to derive. Hence, the authors discuss a solution approach, where at each step the players limit the computation of their actions to a shorter time horizon that may involve only the next few time steps. This moving horizon Nash equilibrium solution proves to be useful in near term decisions of the adversaries. An important extension to this research effort could be accounting for the uncertainty in payoffs by combining robust optimization techniques with game theory.

Game Theory and Robust Optimization

Hayashi et al. (2004) consider a bimatrix game in which the players can neither evaluate their cost functions exactly nor estimate their opponents' strategies accurately. Note that this is the case in many applications in homeland security research. To formulate such a game, authors introduce the concept of robust Nash equilibrium and prove its existence under some mild conditions. Moreover, authors show that a robust Nash equilibrium in the bimatrix game can be characterized as a solution of a second-order cone problem (SOCP). Some numerical results are presented to illustrate the behavior of robust Nash equilibria. Although Hayashi et al. (2004) considered robustness in a bimatrix game, combining robust optimization techniques with game theory is open to many future research areas. First of all, differential or dynamic games with uncertainty could be worthwhile to study through robust optimization techniques. Furthermore, as the authors indicate, the concept of robust Nash equilibrium could be extended to the general N-person game. For the 2-person bimatrix game studied in this paper, it is sufficient to consider the uncertainty in the cost matrices and the opponent's strategy.

To discuss general N-person games, a more complicated structure should be dealt with. Another issue is to find other sufficient conditions for the existence of robust Nash equilibria. Also, theoretical study on the relation between Nash equilibrium and the robust Nash equilibrium is worthwhile. For example, it is not known whether the uniqueness of Nash equilibrium is inherited to robust Nash equilibrium. In this paper, authors have formulated several robust Nash equilibrium problems as SOCPs. However, they have only considered the cases where either the cost matrices or the opponent's strategy is uncertain for each player. According to the authors, it seems interesting to study the case where both of them are uncertain, or the uncertainty set is more complicated. In numerical experiments, authors employed an existing algorithm for solving SOCPs. But, there is room for improvement of solution methods. It may be useful to develop a specialized method for solving robust Nash equilibrium problems.

Game Theory and Reliability

Many of the applications of reliability to security consider the threats against critical infrastructure, such as water supply systems (Haimes, 2002). However, many

applications do not consider an adaptive adversary. Therefore, incorporating game theory and risk and reliability analysis could be a fruitful approach (Bier, 2004).

Hausken (2002) attempts to combine probabilistic risk analysis (PRA) and game theory by associating each unit in a reliability system with a player. By doing so, a behavioral dimension is introduced into PRA framework. The article demonstrates the different conflicts that arise among players in series, parallel, and summation systems over which players incur costs.

Bier et al. (2004) apply game theory and reliability analysis to identify optimal defenses against intentional threats to system reliability. Various scenarios are considered in this paper such as perfect attacker knowledge of defenses and single attack with constrained defender budget or no attacker knowledge and single attack with unconstrained defender budget. Results of this paper emphasize the value of redundancy as a defensive strategy. According to the authors, future research could include extending this work to combinations of parallel and series systems rather than focusing only on pure parallel or series systems. Finding optimal strategies for arbitrary systems is difficult. Hence, near-optimal heuristic attack and defense strategies could be developed. Another promising area of future research is to extend the models to include time, rather than the current static or "snapshot" view of system security. This could allow the modeler to consider imperfect attacker information as well as multiple attacks over time. Another interesting future research topic could be the relation of stochastic games and reliability analysis.

In a more recent effort, Azaiez and Bier (2004) extends results for defense of simple systems to combined series/parallel systems of more realistic complexity. This effort sometimes yields counterintuitive results, such as the observation that defending the stronger components in a parallel subsystem can actually impose greater burdens on prospective attackers than hardening the weaker components. The authors indicate that the approach is limited to cases where the cost of attacks increases linearly with regards to the defensive investments. However, this may hold only for a limited range of defensive investments. Second, an extension could be to relax the budget constraint, and permit the total investment to be optimized based on the value of the system being protected. Third, repeated attacks evolving in time could be investigated.

Stochastic Games

As mentioned in the introduction, unlike naturally occurring or accidental events, terrorism is essentially adversarial. Thus investments designed to protect against one type of terrorism (e.g., against blasts, biological agents, or radiological devices) have the potential to elevate the risk of other types of terrorism over a given time period. An approach that accounts for such an evolution over time could be adopted by using stochastic games.

There is an extensive amount of research in stochastic games in various fields such as economics, mathematics and operations research since the 1950s. The basic two

person zero sum (discrete) stochastic game is played as follows. There are states, and strategy sets for each player and for all states. The system evolves in stages represented by discrete time points. At each state, the system is in one of its states and players 1 and 2 choose their respective actions. There is an immediate payoff as a consequence of the choices of the players. Then, the system moves to another state with some probability according to the previous state, and the choices of the players in the previous state. The fundamental question is then to find the optimal strategies that could be adopted by the players that optimize their own (noncooperative) objectives and the value of the game. Shapley (1953) first introduced stochastic games and proved that the value and optimal strategies of the game exist. Many extensions to this basic model have been proposed after this seminal paper such as games with infinite states and actions, N person games, games with incomplete information, continuous time games, and semi-Markov games among countless others.

Since publications on stochastic games are usually in the form of research papers and monographs, Filar and Vrieze (1997) fulfill a need for the treatment of the topic in a single textbook. The authors study discrete time finite state finite action stochastic games with complete information from the Markov decision processes and mathematical programming point of view, where there are more than one decision maker with conflicting objectives, and use the name ‘Competitive Markov Decision Processes’. The authors treat the discounted stochastic games, its relation with linear programming and nonlinear programming formulations, and the existence of stationary strategies and equilibria in depth. An important result is that the class of nonstationary strategies cannot achieve a better equilibrium value than the class of stationary strategies. Another observation is that, unlike Markov decision processes problems, general two person zero sum stochastic games cannot be solved by linear programming (LP). However, certain restrictions could be imposed on them in order to convert the problem into a suitable linear programming problem. Two of these restrictions are as follows. First, single controller discounted games lend themselves to LPs (Parthasarathy and Raghavan, 1981). In this model, the system makes a transition into the next state with some probability according to the previous state and the action taken by one of the decision makers in the previous state. Hence, the action of the other player is irrelevant in determining the next state. Second, separable-reward-state-independent-transition discounted stochastic games could be converted to an LP. In this model, the payoff function can be expressed by two components, where one component is dependent only on the current state, and the other component is on the pairs of choices made by the decision makers. Also, the transition to the next state is determined only by the pair of actions taken by the opponents and does not depend on the current state of the system (Parthasarathy, et al., 1984).

Advances in stochastic games throughout the years could be viewed from two coupled perspectives: game theoretical perspective, and the stochastic processes perspective.

An extension to stochastic game models mentioned above is the one with incomplete information. The incomplete information case within the repeated games is first introduced by Aumann and Maschler (1968). Several authors have adopted the approach

by Aumann and Maschler (1968) to stochastic games. In a recent paper by Rosenberg, et al. (2004), authors consider stochastic games with incomplete information on one of the players. However, the restriction in this model is that the transitions to the next state are controlled by a single player. Another extension by the same authors concerns incomplete information on both sides. A two-player zero-sum stochastic game with incomplete information is described by a finite collection of stochastic games. It is assumed that the games differ only through their payoffs but they all have the same sets of states and actions, and the same transition matrix. The game is played in stages. A stochastic game is to be played out of the finite set of games over which a probability distribution is specified. Player 1 is informed of the specific game to be played, while player 2 is not. All that the second player knows is that a game is to be chosen randomly from the finite set of games and to be played thereafter. At every stage the two players choose their actions simultaneously and the system moves into the next state. Both players are informed of their actions and the current state of the system. Note that the actual payoff is not told to player 2 but is known by player 1.

It is important to note that the approach adopted by Rosenberg et al. (2004) is based, in some sense, on the approach proposed by Harsanyi (1967, 1968). In his study that brings him the Nobel Prize in 1994, Harsanyi proved that an incomplete two person zero sum normal form game (*I*-game) could be converted into a set of complete information games (*C*-game) that is equivalent to the original *I* game.

Types of extensions to stochastic games from the stochastic processes perspective include considering nonhomogeneous games (Guo and Hernandez, 2004), continuous time games (Laraki and Solan, 2002), semi Markov games (Jaskiewicz, 2002) among numerous others.

Other Approaches

Faria (2004) contends that terrorist innovations result from the innovation effect that is triggered by counterterrorist policies. To model this phenomenon, Faria created a dynamic model of terrorist attacks and innovations. The model consists of a set of differential equations, and is used to compare the effectiveness of three different anti-terrorist policies: deterrence, preemption and intelligence.

Hazen (2002) introduces stochastic trees, where chance nodes in a decision tree can be stochastic nodes. This paper also uses stochastic nodes in influence diagrams. By doing so, variables that change state over time are captured in the influence diagram methodology. The authors apply this new methodology to model medical decisions, and specifically, arthritic joint replacement decisions. An interesting possible extension to this methodology could be considering the use of stochastic nodes in games in extensive forms.

Conclusions and Future Work

The threat of catastrophic terrorism has created a tremendous need for new methodologies to guide strategic investments to protect against adversarial threats. To meet this need, CREATE is developing a family of tools for conducting risk based economic assessments, which can be used to determine which investments are most cost-effective. The work is challenging because the threat is non benign and is capable of adapting and responding to counter terrorist investments.

Section 4.3 introduced a novel approach that combines reliability and game theory, which is open to further research. A future research topic could be adding a time element to the problems introduced by Bier (2004), and Bier et al. (2004). Introduction of dynamics in these problems lends itself to the use of stochastic processes, which provide extensive opportunities for modeling the occurrence of terrorism.

One opportunity for future work will entail application of game theory to the study of adaptive and partially observable adversaries. To this end, applying robust optimization techniques to game theory could be challenging but fruitful as it relies on profound mathematical analysis. Furthermore, handling uncertainty that results from incomplete information about an adversary via robust optimization could be a more realistic approach in strategic planning against an adaptive opponent.

The field of stochastic games lends itself to extensive research opportunities although it readily has a very large body of literature. First that comes to mind could be the study of “robust stochastic games”, which does not exist in the literature, perhaps due to the relatively very short history of robust optimization. Introducing uncertainty sets on the related parameters of the nonlinear programming formulations of stochastic games could result in a novel approach to handling incomplete information. A step towards this could be to study the robustness of single-controller stochastic games since they admit linear programming formulations. It is important to note that single controller games do not entirely meet the requirements imposed by an adversarial opponent since only one player controls the transition probabilities. However, such a study could be a first step and provide insights into the study of general stochastic games through robust optimization.

As explained in detail by Filar and Vrieze (1997), stochastic games are extensions to the Markov Decision Processes. Stochastic dynamic programming is used to solve finite horizon MDPs. The existence of a value and optimal strategies of a stochastic game is already proved by Shapley (1953) and through nonlinear programming by Vrieze (1987). It could be worthwhile to pose the following two questions: What could be achieved by applying stochastic dynamic programming to stochastic games? Could it also be shown that stochastic games admit a unique value and optimal strategies by using stochastic dynamic programming?

Another future investigation might again consider stochastic games with uncertainty on some certain parameters. An alternative way to handle such a problem could be to investigate the use of stochastic optimization instead of robust optimization.

References

1. Atkinson, S. E., Sandler, T., and Tschirhart, J. T. (1987). "Terrorism in a bargaining framework", *Journal of Law and Economics*, Vol.30, No.1.

2. Aumann, R. J., and Maschler, M. B. "Repeated games of incomplete information: The zerosum extensive case", in *Report of the U.S. Arms Control and Disarmament Agency ST-143*,Washington, D.C., 1968, Chapter III, pp. 37–116.

3. Azaiez, N., and Bier, V. M. (2004). "Optimal Resource Allocation for Security in Reliability Systems", Working Paper, Industrial Engineering Department, University of Wisconsin – Madison.

4. Bernard, H. (2004). "Mathematical Methods in Combating Terrorism", *Risk Analysis*, Vol.24, No.4.

5. Bier, V. (2004). "Game-Theoretic and Reliability Methods in Counter-Terrorism and Security", Technical Report, Center for Human Performance and Risk Analysis, University of Wisconsin – Madison.

6. Bier, V., Nagaraj, A., Abhichandani, V. (2004). "Protection of simple series and parallel systems with components of different values", *Reliability Engineering and Systems Safety*, Vol.10, No.27.

7. Brynielsson, J., and Arnborg, S. (2004). Bayesian Games for Threat Prediction and Situation Analysis. Technical Report, Department of Numerical Analysis and Computer Science, Royal Institute of Technology, Stockholm, Sweden.

8. Cruz, Jr., J. B., Simaan M. A., Gacic, A., Liu Y. (2002). "Moving horizon Nash strategies for a military air operation", *IEEE Transactions on Aerospace and Electronic Systems*, Vol. 38, No.3.

9. D'Artigues, A., and Vignolo, T. (2003). "Why Global Integration May Lead to Terrorism: An Evolutionary Theory of Mimetic Rivalry", *Economics Bulletin*, Vol.6, No.11.

10. Faria, J. R. (2003). "Terror Cycles", *Studies in Nonlinear Dynamics & Econometrics*, Vol.7, No.1.

11. Faria, J. R. (2004). "Terrorist Innovations and Anti-Terrorist Policies", Political Economy Working Paper, School of Social Sciences, University of Texas at Dallas.

12. Filar, J., Vrieze, K. (1997). *Competitive Markov Decision Processes*. Springer-Verlag, New York.

13. Guo, X., and Hernandez, O. (2004). "Zero Sum Games for Nonhomogeneous Markov Chains with an Expected Average Payoff Criterion", *Appl. Comput. Math*, Vol. 3, No.1.

14. Haimes, Y. Y. (2002). "Roadmap for Modeling Risks of Terrorism to the Homeland", *Journal of Infrastructure Systems*, June 2002.

15. Haimes, Y. Y. (2002). "Strategic Responses to Risks of Terrorism to Water Resources", *Journal of Water Resources Planning and Management*, Vol.128.

16. Harsanyi, J. C. (1967, 1968). "Games with Incomplete Information Played by Bayesian Players, I-III", *Management Science*, Vol. 14, 159-182, 320-334, 486-502.

17. Hausken, K. (2002). "Probabilistic risk analysis and game theory", *Risk Analysis*, Vol.22.

18. Hayashi, S., Yamashita, N., and Fukushima, M. (2004). Robust Nash equilibria and second-order cone complementarity problems, Technical Report 2004-004, Department of Applied Mathematics and Physics, Kyoto University (April, 2004).

19. Hazen, G. B. (2002). "Stochastic Trees and the StoTree Modeling Environment: Models and Software for Medical Decision Analysis", *Journal of Medical Systems*, Vol.26.

20. Howard, R. A., and Matheson, J.E. (1981). "Influence Diagrams", *Principles and Applications of Decision Analysis*, Vol.2.

21. Hudson, L. D., Ware, B. S., Laskey, K. B., and Mahoney, S. M. (2002) An Application of Bayesian Networks to Antiterrorism Risk Management for Military Planners. Technical Report, Digital Sandbox, Inc.

22. Heal, G., and Kunreuther, H. (2003). "You Only Die Once: Managing Discrete Interdependent Risks", Working Paper Columbia Business School and Wharton Risk Management and Decision Processes Center.

23. Jaskiewicz, A. (2002). "Zero Sum Semi-Markov Games", *SIAM Journal on Control and Optimization*, Vol. 41, No. 3.

24. Koller, D., and Milch, B. (2001). "Multi-agent influence diagrams for representing and solving games", in *Proceedings of the 17th International Joint Conference of Artificial Intelligence.*

25. Kunreuther, H., and Heal, G. (2003). "Interdependent security", *Journal of Risk and Uncertainty,* Vol.26, No.2.

26. LaMura, P. (2000). "Game Networks", in *Proceedings of the 16th Conference on Uncertainty in Artificial Intelligence.*

27. Lapan, H. E., and Sandler, T. (1988). "To bargain or not to bargain: That is the question." *American Economic Review*, Vol.78, No.2.

28. Lapan, H. E., and Sandler, T. (1993). "Terrorism and signaling", *European Journal of Political Economy*, Vol.9, No.3.

29. Laraki, R., and Solan, E. (2002). "Stopping Games in Continuous Time", *SIAM Journal on Control and Optimization*, to appear.

30. Laskey, K. B. and Levitt T. S. Multisource Fusion for Opportunistic Detection and Probabilistic Assessment of Homeland Terrorist Threats. (2002) Technical Report, SEOR Department, George Mason University.

31. Major, J. (2002). "Advanced techniques for modeling terrorism risk", *Journal of Risk Finance,*Vol.4.

32. Parthasarathy, T., and Raghavan, T.E.S. (1981). "An Orderfield Property for Stochastic Games When One Player Controls Transition Probabilities", *Journal of Optimization Theory and Applications*, Vol. 33, 375-392.

33. Parthasarathy, T., Tijs, S.H., and Vrieze, O. J. (1984). "Stochastic Games with State Independent Transition and Separable Rewards", Selected *topics in OR and Mathematical Economics*. Springer-Verlag, Lecture Note Series 226, New York.

34. 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.

35. Pearl, J. (1988). *Probabilistic Reasoning in Intelligent Systems: Networks of Plausible Inference*, Morgan Kaufmann Publishers, San Francisco.

36. Rosenberg, D., Solan, E., and Vieille, N. (2004). "Stochastic Games with a Single Controller and Incomplete Information", *SIAM Journal of Control and Optimization*, Vol. 43, No.1.

37. Sandler, T., and Arce M., D. G. (2003). "Terrorism and Game Theory", *Simulation & Gaming*, Vol.34, No.3.

38. Sandler, T., Tschirhart, T. T., and Cauley, J. (1983). "A theoretical analysis of transnational terrorism", *American Political Science Review*, Vol.77, No.4.

39. Sandler, T., and Siqueira, K. (2002). “Global terrorism: Deterrence versus preemption”. Unpublished manuscript, University of Southern California.

40. Shachter, R. D. (1986). “Evaluating influence diagrams”, *Operations Research*, Vol.34, No.6.

41. Singh, S., Tu, H., Allanach, J., Pattipati, K.R., and Willett, P. (2004). “Stochastic Modeling of a Terrorist Event via the ASAM System”, in *Proceedings of the International Conference on Systems, Man and Cybernetics*, The Hague, The Netherlands.

42. Shapley, L.S. (1953). “Stochastic Games”. *Proceeding of the National Academy of Science*, 39, 1095-1100.

43. Virtanen, K., Karelahti, J., Raivio, T., and Hamalainen, R. P. (2004). Modeling Air Combat by a Moving Horizon Influence Diagram Game, Technical Report, Systems Analysis Laboratory, Helsinki University of Technology, Finland.

44. Virtanen, K., T. Raivio, R. P. Hämäläinen. (2004b). “Modeling pilot’s sequential maneuvering decisions by a multistage influence diagram”, to appear in *Journal of Guidance and Control*.

45. Vrieze, O. J. (1987). “Stochastic Games with Finite State and Action Spaces”, CWI Tracts 33, Amsterdam.

46. Weaver, R., Silverman, B. G., Shin, H., and Dubois, R. Modeling and Simulating Terrorist Decision-Making: A “Performance Moderator Function Approach to Generating Virtual Opponents.” 10th Conference On Computer Generated Forces and Behavioral Representation, SISO, May, 2001.