Journal of Homeland Security and Emergency Management

Volume 8, *Issue* 1 2011 *Article* 15

Optimal Blends of History and Intelligence for Robust Antiterrorism Policy

Maciej M. Latek, *George Mason University*
Seyed M. Mussavi Rizi, *George Mason University*
Tariq A. Alsheddi, *King Fahd Security College*

Recommended Citation:
Latek, Maciej M.; Mussavi Rizi, Seyed M.; and Alsheddi, Tariq A. (2011) "Optimal Blends of History and Intelligence for Robust Antiterrorism Policy," *Journal of Homeland Security and Emergency Management*: Vol. 8: Iss. 1, Article 15.
DOI: 10.2202/1547-7355.1795
Available at: http://www.bepress.com/jhsem/vol8/iss1/15

©2011 Berkeley Electronic Press. All rights reserved.

Optimal Blends of History and Intelligence for Robust Antiterrorism Policy

Maciej M. Latek, Seyed M. Mussavi Rizi, and Tariq A. Alsheddi

Abstract

Antiterrorism analysis requires that security agencies blend evidence on historical patterns of terrorist behavior with incomplete intelligence on terrorist adversaries to predict possible terrorist operations and devise appropriate countermeasures. We model interactions between reactive, adaptive and intelligent adversaries embedded in minimally sufficient organizational settings to study the optimal analytic mixture, expressed as historical memory reach-back and the number of anticipatory scenarios, that should be used to design antiterrorism policy. We show that history is a valuable source of information when the terrorist organization evolves and acquires new capabilities at such a rapid pace that makes optimal strategies advocated by game-theoretic reasoning unlikely to succeed.

KEYWORDS: antiterrorism, multiagent simulation, intelligence analysis, anticipatory thinking

Author Notes: Alsheddi thanks King Fahd Security College and the Prince Naif Chair for Intellectual Security at King Saud University for partially funding this project.

1 Introduction

1.1 The Problem

Antiterrorism analysis requires that security agencies blend incomplete intelligence on terrorist adversaries with evidence on their historical behavior to predict possible terrorist operations and devise appropriate countermeasures. Mixing intelligence and historical information to obtain robust predictions is hardly confined to antiterrorism. For example, foreign exchange *fundamentalism* relies on economic news to form expectations of future exchange rates while *chartism* predicts exchange rates as some function of their historical values. Fundamentalism relegates history to irrelevance while chartism holds historical regularities supreme. However, foreign exchange analysts mix information from both sources to predict exchange rates. For instance, 60% of analysts in London foreign exchange markets reported that they considered charts no less important than fundamentals for short-run predictions (Taylor and Allen 1992).

What is the proper analytic mix of intelligence and history that offers security agencies robust antiterrorist measures? To answer this question, we build a multi-agent model in which a terrorist cell and a security agency interact in a complex, non-zero-sum setting for an extended period of time and anticipate each other's moves by using recursive simulation and a cognitive hierarchy model. The terrorist cell launches complex attacks against specific targets. The security agency allocates static defenses to each target and mobile defenses to all targets. The model features a terrorist organization that achieves diversion by launching multi-stage attacks to overwhelm antiterrorists' decision making procedures (Heuer 1981); different paths to operational failure in the terrorist organization (Fishman 2009; Jackson and Frelinger 2009), and *strategic uncertainty* about which equally good strategy each adversary chooses (Crawford and Haller 1990).

1.2 Literature Review

Four types of questions fare prominently in the game-theoretic modeling of terrorism: (a) Allocation of a fixed budget by the government to counter attacks against potential targets; (b) offensive and defensive countermeasures by the government; (c) asymmetric information and secrecy, and (d) interaction between political and militant factions of terrorist groups (Sandler and Siqueira 2008). These questions are answered by generally unique equilibrium outcomes of a sequential game in which a defender decides how much to spend on defense and where to spend it on first. The more a defender dedicates to hardening or protecting a potential target, the less likely an attack on that target is to succeed. After the defender moves,

the terrorist group chooses how much effort or resources to devote to attacking the defender and how to allocate that effort to possible targets. The more effort the terrorist group devotes to a target, the more likely the attack on the target is to succeed. This approach works under full or partial information where the government hides or reveals information to sway the terrorist organization to or away from a specific target (Powell 2008). In this setting, governments can benefit from openness through improved analysis and coordination among security agencies under some conditions (Powell 2007). Noisy intelligence and the necessity to defend against multiple types of attackers also lead to partial intelligence, tackled by Bayesian methods reported in Tsai et al. (2009; 2008).

Game-theoretic solutions to a, b, c and d account for an intelligent adversary and differ from solutions derived against a non-strategic adversary modeled as nature (Brown et al. 2008; McLean et al. 2008). However, this advantage comes at significant costs: Firstly, algorithms for finding game-theoretic equilibria are computationally feasible only in stylized environments with relatively simple action sets (Daskalakis et al. 2006). Game theory has only recently begun to address multiperiod, repeated interactions (Zhuang et al. 2010), bounded rationality and perception (Hao et al. 2009; Jenelius and Holmgren 2009). Secondly, game-theoretic approaches can model neither evolving nor interacting organizations. Multiagent simulations on the other hand, can model evolving *and* interacting terrorist and antiterrorist organizations in complex environments characterized by policy relevant information and behavioral constraints (Jackson and Frelinger 2009). Yet, existing multiagent models of terrorism (Schreiber et al. 2004; Parunak et al. 2009) are limited to terrorist organizations with purely heuristic agents or those that reason only about their own organization and the tasks at hand.

We demonstrate that our model not only answers questions $a, b,$ and c, but also goes beyond game-theoretic analysis by producing strategies that are robust to strategic uncertainty and execution errors. We will introduce an antiterrorism case study to shed light on the conditions under which defending against history yields better results than defending against predictions based on intelligence on a terrorist organization, arguing that the evolving structure of a terrorist organization weakens the usefulness of anticipatory solutions advocated by game theory.

2 The Model

2.1 General Concepts

The key challenge to antiterrorists who face adaptive and intelligent adversaries is to obtain mixtures of history and intelligence that predict the most likely and effective

terrorist operations, and to determine which of their own countermeasures is robust to strategic uncertainty and to replanning contingencies.

Strategic uncertainty arises when decision makers grapple with adversaries who enjoy multiple, equally desirable strategies. Inaccurate intelligence exacerbates strategic uncertainty for antiterrorists; however, accurate intelligence does not solve the problem. For example, knowing for certain that Al-Qaeda is indifferent between operations X, Y and Z does not help to predict the operation it will launch. Forces of nature, adversary disruption and inaccurate intelligence compel both terrorists and antiterrorists to replan mid-course. However, replanning contingencies affect terrorists who often operate with marginally adequate resources under time pressure differently from antiterrorists who may be lulled into organizational complacency.

To derive optimal analytical mixtures under strategic uncertainty and replanning contingencies, the model is divided into a tactical model and a cognitive architecture for robust strategic reasoning. The tactical model consists of a minimally sufficient representation of the environment and a multiagent model of non-strategic organizational behavior. It simulates the production stage of terrorist operations in which terrorist operatives decompose operations into tasks and negotiate task delegation and execution among themselves. It also determines operational outcomes for both terrorists and antiterrorists given the strategy each has committed to. Next, we describe an implementation of our approach to robust strategic reasoning.

2.2 Recursive n-th Order Rationality

In order to choose a strategy, terrorist ring leaders and antiterrorist decision makers ask what-if questions to *reason* about how interactions of their strategies shape the future. Our implementation of this reasoning process uses *multiagent recursive simulation* (MARS) and *n-th order rational agents* (NORA) as core technologies. In MARS, anticipatory agents populate a tactical model they have *cloned* and simulate the world forward in the cloned model to determine outcomes of their strategy and to best respond to opponents' strategies by optimizing over their own strategy space. We deal with endemic symptoms of the world of antiterrorism such as secrecy, cognitive distortions and information impartiality by a noisy cloning of the environment that does not result in an exact replica of the environment. NORA is a best response mechanism for anticipatory agents that is based on a hierarchy of rationality levels. In order to best respond to adversaries' strategies, terrorists and antiterrorists need to form expectations of each other's strategies. They do so by assuming a cognitive hierarchy of rationality levels in which agents at each level best respond to adversaries whom they assume are one level less rational. At level zero, agents follow historical or expert-designed strategies.

Purely anticipatory thinking may hamstring antiterrorists with overwhelming strategic uncertainty, if intelligence on terrorists' preferences and organizational behavior and structure is incomplete. To curtail strategic uncertainty, antiterrorists can combine data on past terrorist operations with expectations of future operations derived through MARS–NORA. Next, we determine proportions of historical information and intelligence analysis called *analytical mix* that should be weighted by antiterrorists to design strategies that are robust to strategic uncertainty and execution contingencies.

2.3 Notation

In the Appendix we detail an algorithm for the MARS–NORA cognitive architecture. In Section 3 we map a real-life case study onto the structure of our simulation and elaborate the mechanics of the tactical model. Here we provide a list of MARS–NORA key parameters: R denotes the terrorist ring leader and B the antiterrorist decision maker; d_R and d_B denote depth of recursive reasoning; h_R and h_B planning horizon in days; τ_R and τ_B the number of forward looking strategies derived by n-th order rational reasoning, and finally κ_R and κ_B the number of the most recent historical scenarios for the terrorist ring leader and the antiterrorist decision maker. R maximizes his expected payoffs over the next h_R simulation days by best responding to $\tau_B + \kappa_B$ of B's strategies derived by d_B. Likewise, B maximizes his expected payoffs over the next h_B simulation days by best responding to $\tau_R + \kappa_R$ of R's strategies derived by d_R.

3 Case Study

We use MARS–NORA to create a model of the 1995 car bomb attack on the Vinnell Corporation offices in Riyadh as a case study to answer our research question. We first recount the actual case and then detail our model of organizational behavior and strategic interaction between terrorists and security forces.

3.1 The Real Story

Former Jihadi Saudis who had trained in Afghanistan, Aziz (AZ), Musleh (MS), Ryiadh (RD), and Khalid (KD) planned a terrorist attack in Riyadh the capital of the Kingdom of Saudi Arabia (KSA) in 1995.[1] Figure 1 shows the group composition.

[1]This description of the attack is based on open source accounts of the attack by the Saudi media. Terrorist preferences and operational payoffs are based on interviews with security experts with a keen knowledge of the case. The data and narratives are available upon request.

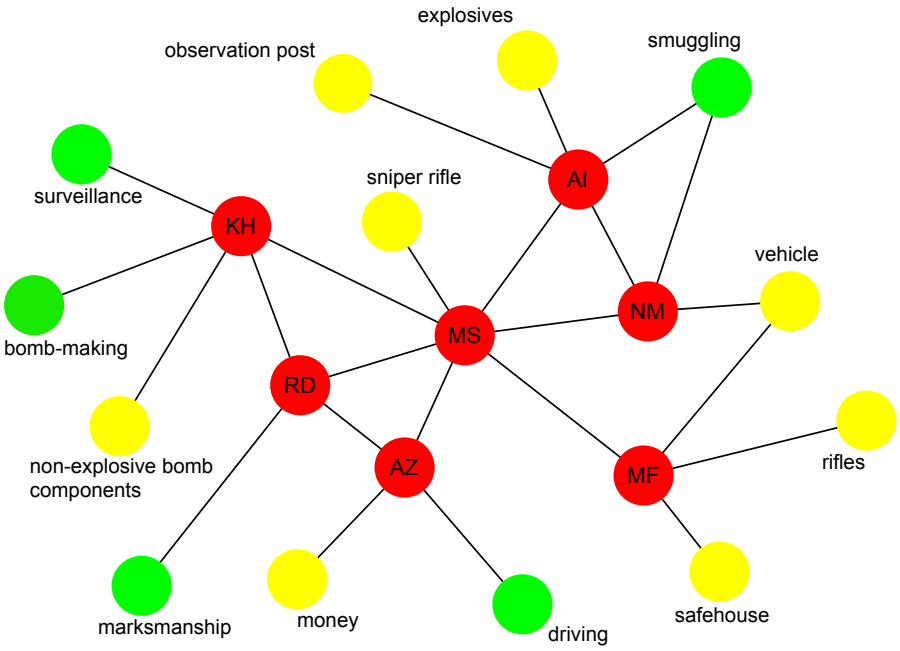

Figure 1: Initial view of the terrorist cell. AZ is a Strategist using MARS–NORA to design operations. The remaining agents are Operatives using the BDI architecture and hierarchical task network decomposition. Legend: ● agent, ● skill, ● resource.

The cell compiled a list of targets consisting of the Ministry of Defense (MOD), Ministry of Media (MOM), Terrorism Investigation Unit (TIU), the American Embassy (AE) and Vinnell Corporation (VC) offices and considered different modes of attack, ranging from sniping and raids to hostage taking and vehicle-borne IED (VBIED). The cell decided on a VBIED attack on the VC offices after evaluating various operations in terms of target hardness and the political impact of a successful operation, as shown in Table 1. The group spent a month on surveillance, studying the location, its entrance and exits and guard shifts. A week before the attack, Aziz and Musleh traveled to Yemen, bought 200 Kg of TNT from a Yemeni national Ali (AI), smuggled it back to the KSA with the help of another Yemeni national Nomaan (NM), and stored it in a safehouse close to the city of Riyadh. Meanwhile Riyadh acquired and prepared an old pickup truck as the IED vehicle and drove it to the safehouse. The terrorists loaded the explosives onto the IED vehicle the night before the attack. On the day of the attack, Khalid and Riyadh left the safehouse in the IED vehicle. Musleh and Aziz followed the IED vehicle

in Musleh's car. At the location, Khalid parked the IED vehicle without attracting attention and set the IED timer. The four drove away in Musleh's car.

Target	Mode of attack				Hardness
	VBIED	Sniping	Trash bombing	Raiding	
VC	$\begin{pmatrix} 10 & -10 \\ -3 & 1 \end{pmatrix}$	*	$\begin{pmatrix} 2 & -2 \\ -2 & 1 \end{pmatrix}$	$\begin{pmatrix} 3 & -3 \\ -4 & 1 \end{pmatrix}$	1
MOM	$\begin{pmatrix} 20 & -10 \\ -3 & 1 \end{pmatrix}$	*	$\begin{pmatrix} 2 & -2 \\ -2 & 1 \end{pmatrix}$	$\begin{pmatrix} 6 & -6 \\ -4 & 1 \end{pmatrix}$	2
MOD	*	$\begin{pmatrix} 1 & -1 \\ -2 & 1 \end{pmatrix}$	*	*	5
AE	$\begin{pmatrix} 40 & -40 \\ -3 & 1 \end{pmatrix}$	$\begin{pmatrix} 1 & -1 \\ -2 & 1 \end{pmatrix}$	*	*	4
TIU	*	$\begin{pmatrix} 2 & -1 \\ -2 & 1 \end{pmatrix}$	$\begin{pmatrix} 3 & -3 \\ -2 & 1 \end{pmatrix}$	*	3

Table 1: In $\left(\begin{smallmatrix} a & b \\ d & c \end{smallmatrix}\right)$, a and b are terrorist cell and KSAS payoffs respectively if an operation succeeds; c and d are terrorist cell and KSAS payoffs respectively if an operation fails. * means that the operation is not applicable to the target. The last column describes the inherent ease of securing the target.

3.2 MARS–NORA Model of the Vinnell Case

Any MARS–NORA model that explicitly models organizational behavior consists of strategic agents who anticipate each other's strategies by reasoning about their own and their opponent's capabilities and payoffs associated with adopting different strategies, and tactical agents who carry out operations conceived at the strategic level by matching people, resources and information required to perform each operational task and by performing those tasks once required resources are available. Our rendition of the VC car bomb case consists of Aziz and KSA Security (KSAS) as *Strategists*. Aziz uses MARS–NORA to determine sets of $\langle \text{target}, \text{attack mode} \rangle$ pairs called operations for the terrorist organization. Most of Aziz's operations are multi-stage, in which a small precursor attack is used to divert KSAS mobile defenses before the main attack. The remaining agents in the terrorist cell are *Operatives* who communicate with each other and muster resources to perform the

tasks necessary to successfully execute the operation designated by Aziz. After Aziz chooses an operation, he turns into an Operative and acts as such until the operation succeeds or fails. KSAS uses MARS–NORA to allocate static defense forces to each target and generate mobile defense forces that are not tied to any specific target, given its budget constraint.

The terrorist cell and KSAS receive payoffs every time an operation succeeds or is foiled by KSAS. Suppose the cell manages to organize an operation aimed at target c, with hardness x_c while KSAS allocates s_c to the static defense of this target and m to mobile forces that contribute to the security of any site by a factor of y. The probability that the operation succeeds is $1/\{1+\exp[x_c(s_c+ym)]\}$. Depending on the outcome of the attack, the cell and KSAS receive payoffs according to Table 1. Regardless of the outcome of an attack, mobile forces are depleted by a fraction α and are replenished at the rate β at any period the terrorist cell does not attempt an operation.

Inspired by the belief-desire-intention (BDI) architecture (Rao and Georgeff 1991), we modeled Operatives similar to those in Tsvetovat and Łatek (2009). Here, *desires* are the operations that the terrorist organization decides to launch, for example VBIED the AE; *intentions* are the intermediary tasks it should carry out in order to execute the operation, for example conducting target surveillance, and *beliefs* contain an Operative's information about his own resources and skills and those of other agents. The ontology of an Operative's beliefs is the same as that of the initial state of the terrorist cell. This condition allows Aziz and KSAS to clone and populate the world based on their private information, and evolve their strategies in response to changing beliefs.

The BDI architecture of Operatives is accompanied by a behavioral logic provided by hierarchical task network decomposition (Tate 1977) that determines the sequence of intermediate steps required to fulfill task dependencies for any operation. Shown in Figure 2, the hierarchical task network of all operations considered in the scenario is part of public information available to all agents and highlights operational tasks an agent cannot perform himself. In this case, an Operative can probe other Operatives for a resource or information he lacks; receive the requested resource or information, if provided with them; delegate tasks to other Operatives; receive a task and report if it was carried out successfully, and introduce two other Operatives to each other. Operatives update their beliefs every time a bit of information is exchanged within the terrorist cell. If an Operative cannot find a way to execute a task, he reports a time-out and requests that Aziz choose a new operation.

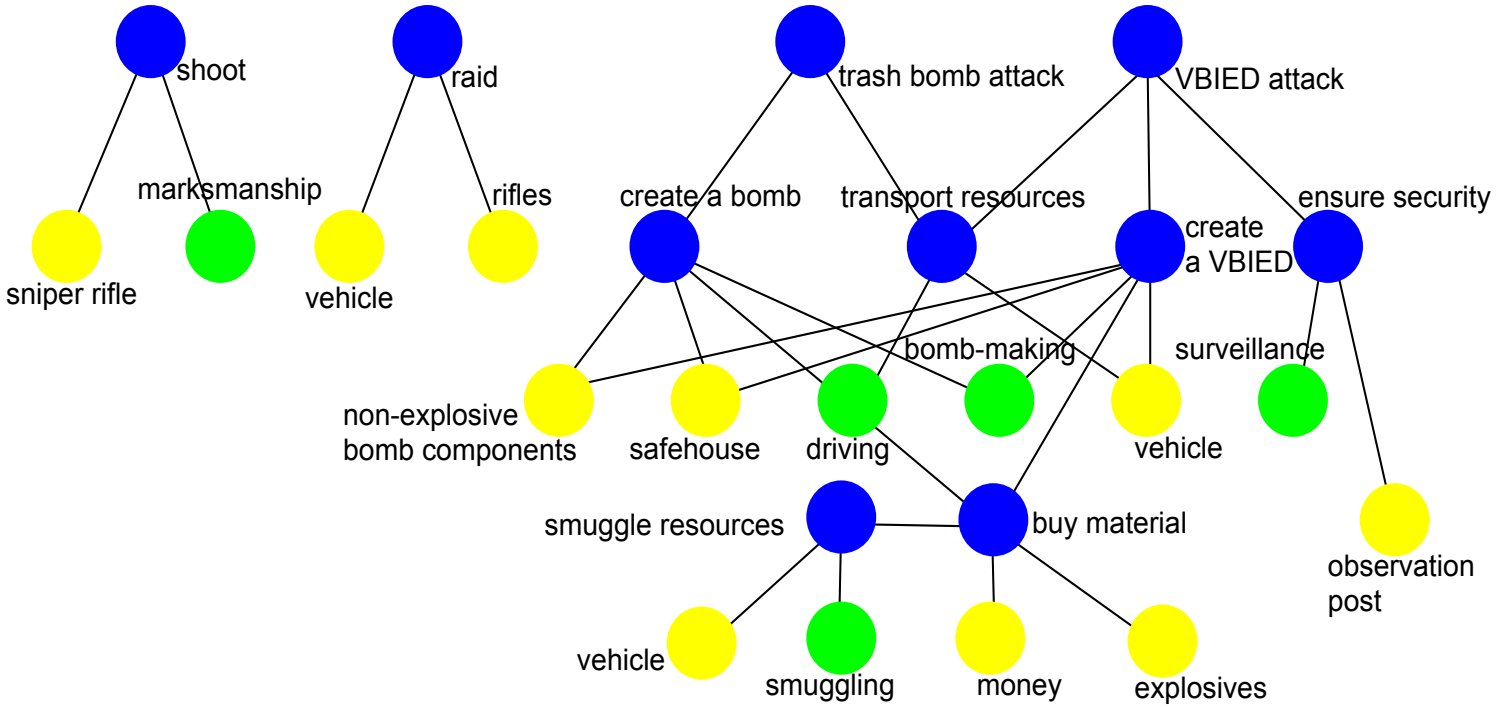

Figure 2: Graph of plan-target dependency. Legend: skill, resource, tasks.

Figure 1 shows the initial objective view of the terrorist cell, including agent-agent, agent-resource, and agent-skill networks. Initially, terrorist agents do *not* have access to this picture, since their beliefs are initialized with their first-degree neighbors. More importantly, KSAS is not even aware of the existence of the terrorist cell at first. Figure 2 shows dependencies for operations that can be conceived by Aziz, including task-resource and task-skill networks. Aziz knows which targets each operation applies to and what losses a successful operation may impose on KSAS as listed in Table 1, but does not know if his organization can carry out any of the operations. He also needs to account for the KSAS force allocation to each target and mobile patrols across the city of Riyadh. So an operation may fail because of miscoordination among the members of the terrorist cell, forces of nature or both. It may also be foiled by KSAS. If Aziz determines the cell capabilities and KSAS defenses make it impossible to stage a successful operation, he may not attempt anything until he learns a new fact about his team or the state of the world, or until KSAS changes its defensive posture.

In the language of MARS–NORA, Aziz uses $d_R = 1, h_R = 50$ and $\tau_R = 1$ where $d_R = 1$ means that he best responds to KSAS; $h_R = 50$ shows that he conceives a long planning horizon of 50 days so that he can make temporal tradeoffs among resources used in each operation, the endogenous likelihood of failure and outcomes for more than one operation. Finally, $\kappa_R = 1$ indicates that he considers only the last defensive allocation of KSAS. Regardless of whether they succeed or not, all terrorist operations provide KSAS with bits of information that it will use to simulate the terrorist organization. When designing a defensive policy, KSAS uses not only the last $\kappa_B = 5$ operations of the terrorist cell, but also anticipates the future operations by Aziz's cell with $d_B = 2, h_B = 50, \tau_B = 5$ in order to hedge against strategic uncertainty.

In the next section, we will describe how KSAS performance and types of defensive allocation depend on the mixture of τ and κ it applies to designing defensive policy.

4 Results

4.1 Experimental Design

We ran experiments that measured changes in the performance of KSAS when it applied various mixtures of history and anticipation to respond to the terrorist cell. We kept the rationality orders of strategic agents fixed, with Aziz playing first-order rational, Stackelberg best response $d_R = \tau_R = 1$, and the KSAS playing second-order rational $d_B = 2$. KSAS analyzes scenarios as tuples of targets and modes of

attack. κ_B scenarios come from the history of interactions between KSAS and the terrorist cell; others are provided by τ_B forward-looking simulations of the terrorist cell by KSAS. We will assess how mixtures of history and anticipation affect the KSAS payoff stream as a function of its budget and the number of past interactions between the opponents. We kept the rest of the model parameters, summarized in Table 2, constant. We perform sensitivity analyses on our results by sweeping KSAS operational security and budget levels once we identify reasonable values for analytical mix.

Parameter	**Scenario value**	**Meaning**
$d_R, h_R, \tau_R, \kappa_R, K_R$	$1, 50, 1, 0, 10$	Aziz's order of rationality, planning horizon, forward-looking samples, historical samples, and number of iterations.
d_B, h_B, K_B	$2, 50, 10$	KSAS order of rationality, planning horizon and number of iterations.
$\langle \tau_B, \kappa_B \rangle$	$\in (0, 10) \times (0, 10)$	KSAS analytical mixture.
γ	$\in \{0.5, 1.5, 2.5\}$	KSAS budget.
δ	$\in [0, 2]$	Operational security as noise added to the perception of KSAS policy by the terrorists.
y	1.0	Contribution of mobile defense to site security.
α	0.25	Damage to mobile defenses in an attack.
β	0.1	Replenishment rate for mobile defenses.
Intercept probability	0.005	Probability of message intercept.

Table 2: Parameter values used in experiments.

4.2 Optimal Analytical Mix

Figure 3 presents average instantaneous loss rates for KSAS on days $50, 250, 450, 650, 850$ and 1050 as a function of the analytical mixture $\langle \tau_B, \kappa_B \rangle$ that it adopts and the budget of 1.5. Initially, KSAS has neither sufficient past cases nor intelligence to design an effective defensive policy. After some 250–500 days, optimizing against historical cases provides sufficient information for KSAS to capture the broad structure of the environment and to determine the targets it should defend with static or mobile defense. However, the terrorist organization is still evolving and acquiring new capabilities, making the KSAS anticipation of its next targets difficult if not counterproductive. In the long run, KSAS obtains optimum results by combining a moderate number of historical cases (5) with a large number of forward-looking scenarios (10) that predict the tactical behavior of the terrorist cell.

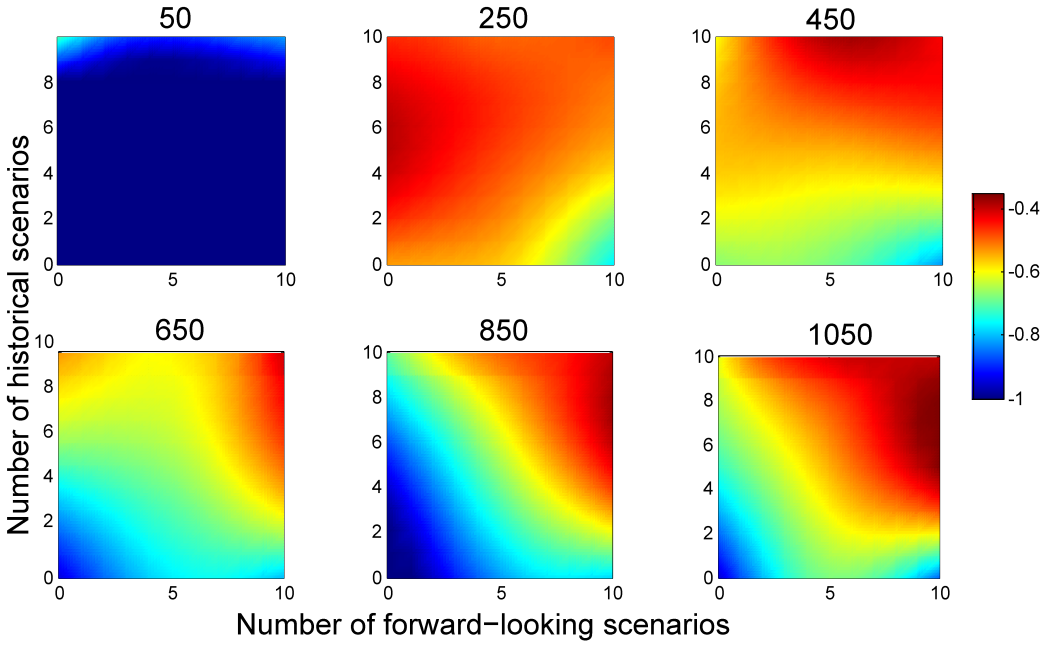

Figure 3: KSAS payoffs on days $50, 250, 450, 650, 850$ and 1050 as a function of analytical mixture with KSAS budget of 1.5. We plot the size of a set of historical scenarios κ_B on the y-axis and the number of forward-looking samples τ_B on the x-axis.

Figure 4 presents the dynamics of observed versus predicted KSAS payoffs when it only optimizes against historical patterns of attack by the terrorist cell $\langle \tau_B, \kappa_B \rangle = \langle 0, 10 \rangle$; disregards such patterns and relies on anticipation alone $\langle \tau_B, \kappa_B \rangle = \langle 10, 0 \rangle$ and emphasizes history and anticipation equally $\langle \tau_B, \kappa_B \rangle = \langle 5, 5 \rangle$. Re-

gardless of the analytical mixture KSAS adopts, it consistently produces overly optimistic predictions about its own payoffs. This optimism bias stems from the narrow variety of attack types the terrorist cell can initially launch and the failure of forward-looking scenarios to confirm that the terrorist organization can plausibly execute an operation. If the variety of operations is small, KSAS can hedge against all of them with some budgets. Yet, the budget of 1.5 forces KSAS to make trade-offs among targets, because it cannot defend *all* of them effectively against some combinations of attack types. The terrorist cell observes and exploits these trade-offs. KSAS adapts to the new situation after some time by reallocating defenses to targets. This limited-resources dynamic gives rise to cycles in the observed payoffs for KSAS, shown on Figure 4, that persist even in the long run when KSAS has come to know the non-evolving terrorist organization completely.

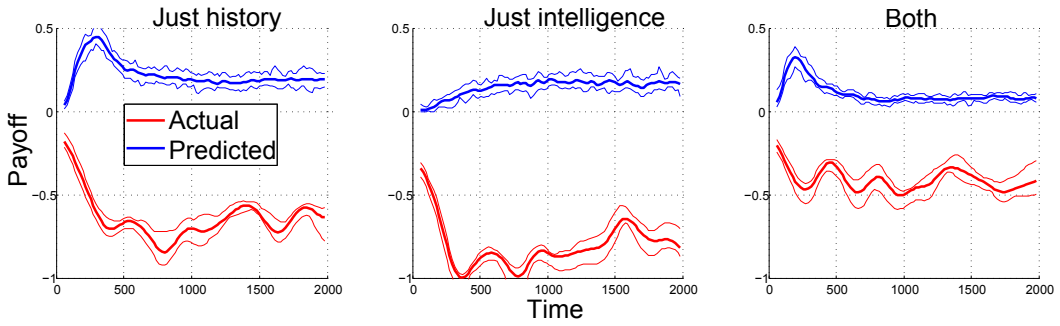

Figure 4: Predicted versus actual payoffs for KSAS for different analytical mixtures and budget of 1.5. When KSAS only optimizes against historical patterns of attack by the terrorist organization we set $\langle \tau_B, \kappa_B \rangle = \langle 0, 10 \rangle$; when it disregards such patterns and relies on anticipation alone we set $\langle \tau_B, \kappa_B \rangle = \langle 10, 0 \rangle$ and when it emphasizes history and anticipation equally we set $\langle \tau_B, \kappa_B \rangle = \langle 5, 5 \rangle$.

4.3 Secrecy and Budget Level

Limited budget makes it impossible for KSAS to hedge against strategic uncertainty, even though proper analytical mixtures account for the uncertainty associated with intelligence on the terrorist organization. Under a reasonable analytical mixture $\langle \tau_B, \kappa_B \rangle = \langle 5, 5 \rangle$, relaxing the budget constraint enhances the performance of KSAS. Two less intuitive results, presented on Figure 5, relate the effect of KSAS budget on its force allocations to each target: The ratio of forces allocated to mobile defense shrinks with the possibility of diversionary attacks. For small budgets, KSAS does not attempt to equalize the expected payoffs of the terrorist organization over different targets, since the environment contains targets of different value

and hardness *and* the game is non-zero-sum. Instead, it leaves some targets exposed in order to protect those it values more than the terrorist organization. Additionally, KSAS rank-allocates forces to targets instead of scaling up allocations proportionally.

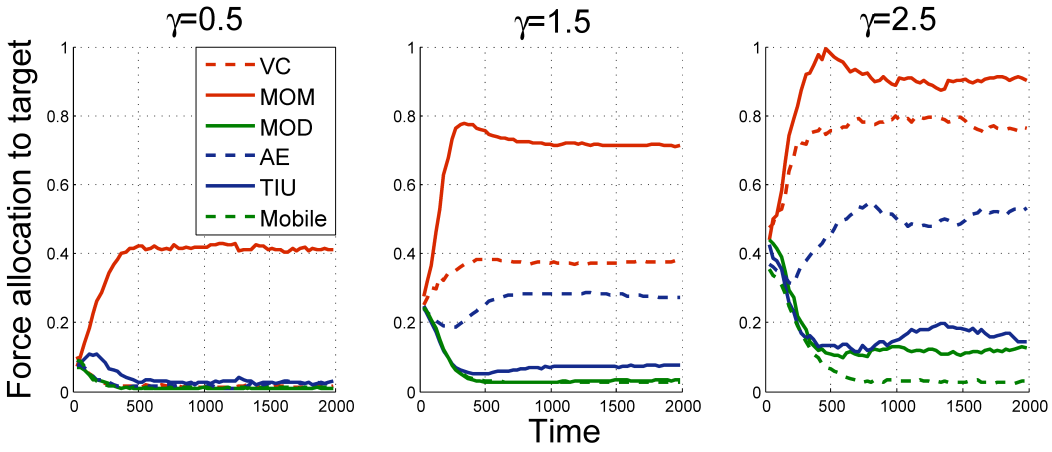

Figure 5: Absolute value of KSAS defensive allocations to each of the targets and mobile defenses as a function of time for budgets $\gamma = 0.5, 1.5, 2.5$ under analytical mixture $\langle \kappa_B, \tau_B \rangle = \langle 5, 5 \rangle$.

KSAS budget also impacts the effectiveness of its operational security as a proxy for secrecy. We define KSAS operational security as the accuracy with which Aziz can measure the KSAS defensive allocation. We add noise uniformly drawn from $[0, \gamma\delta]$ to the actual KSAS budget allocation to each target, then renormalize the sum of Aziz's noisy perceptions back to γ where γ is the KSAS budget and $\delta \in [0, 2]$ is the scaling parameter of the distribution. Figure 6 presents the probability that a terrorist operation that goes past the production stage is successful in penetrating KSAS defenses. This probability always decreases as KSAS operational security increases. As KSAS operational security affects the $\langle$target, attack type$\rangle$ mixture, decreases in the proportion of attacks that can penetrate KSAS defenses does not necessarily translate into minimizing KSAS losses. For constrained budgets like $\gamma = 0.5$, we observe that increasing operational security up to slightly above 1 is counterproductive, and shows little effect for values higher than 1. The intuition behind this result indicates the value of KSAS force allocation to each target as a signaling mechanism to the terrorist cell. As the terrorists' perception of the KSAS force allocation becomes more noisy, the probability of their success for each operation plummets. However, KSAS also loses because it does not have enough budget to harden higher value targets, so most of terrorists' failures are over

targets that KSAS does not value all that much, while the terrorists' successes coalesce disproportionately around randomly chosen operations that hurt KSAS the most.

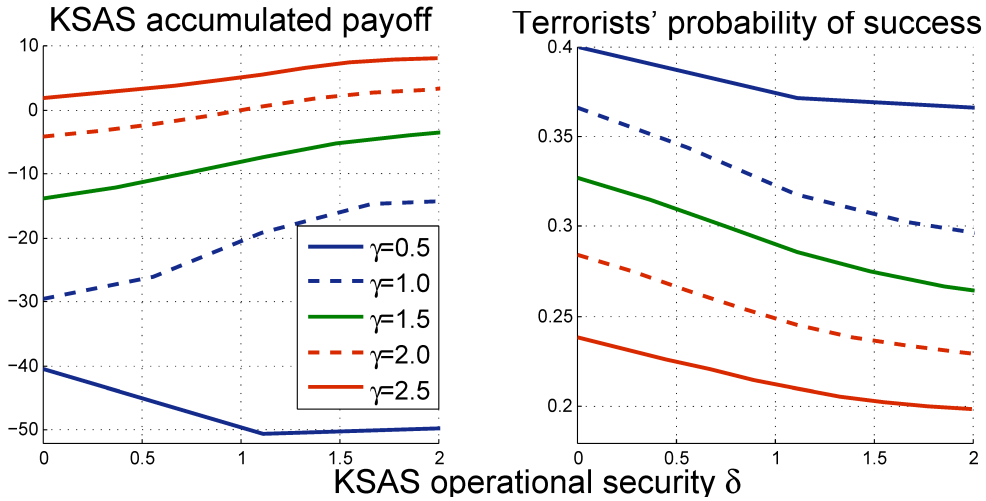

Figure 6: The impact of KSAS operational security under analytical mixture $\langle \kappa_B, \tau_B \rangle = \langle 5, 5 \rangle$ for different budget levels. KSAS payoff is accumulated over 2000 simulated days. Terrorists' probability of success is measured for each operation that successfully completed the production stage.

5 Conclusions

We have created a model that features interactions among reactive, adaptive and intelligent adversaries in an organizational setting. It gives security forces and the terrorist organization a minimally sufficient model of organizational behavior; characterizes strategic interactions between the opponents in which each adversary uses a behavioral game-theoretical model to adjust its strategies based on its expectation of what the opponent will do, and makes terrorism risk assessment possible for repeated interactions among multiple, distinct security and terrorist organizations by multiagent recursive simulation. We examined the issue of optimal analytic mixture that should be used to design antiterrorism strategy, expressed as historical memory reach-back and the number of anticipatory scenarios. History proved to be a valuable source of information when the terrorist organization evolves and acquires new capabilities at such a rapid pace that makes optimal strategies advocated by game-theoretic reasoning unlikely to succeed. Taking only history into account is

generally sufficient to distinguish which targets are of value to both sides and what actions and counteractions proved to be effective.

Appendix: Multiagent Modeling of Strategic Decisions

In this appendix, we describe the inner workings of multiagent recursive simulation (MARS) and n-th order rational agents (NORA), and outline algorithms that use MARS to derive robust myopic strategies for NORA.

Building Blocks

Assume a model $\mathbf{\Psi}$. For $\mathbf{\Psi}$ to be useful for modeling strategic interactions, it needs to fulfill a few simple conditions regardless of whether it is a multiagent model of interactions among purposive agents or a statistical model that simply predicts outcomes as functions of inputs. First, observe that the primary value of $\mathbf{\Psi}$ is in scenario analysis, because $\mathbf{\Psi}$ defines the joint strategy space for all agents, and the states of the environment for any realization of the joint strategy space. If $\mathbf{\Psi}$ is to be used to model strategic interactions, it should also describe how agents value the world by calculating agents' payoffs for any trajectory of interactions among them, using a scoring mechanism based on their implicit or explicit preferences or utilities. Per definition, any multiagent or game-theoretic model fulfills these conditions (Axtell 2000). Other approaches may need to be augmented with an accounting mechanism that translates realizations of the joint strategy space and predicts states of the environment into outcomes for individual actors. Lastly, $\mathbf{\Psi}$ can conveniently store information about past agent interactions in a library of historical interactions among agents called historical behaviors library (HBL). If no actual information is available, HBL is either empty or filled with hypothetical expert-designed interaction scenarios.

A strategic agent with knowledge of such a $\mathbf{\Psi}$ can (1) clone it, (2) initialize it with his perception of the current state of the environment, and (3) simulate the world forward in the cloned $\mathbf{\Psi}$, optimizing over strategies that meet his objectives. When applied to multiagent models, this recursive approach to decision making amounts to having simulated decision makers use optimization and simulation to choose strategies (Gilmer 2003) and constitutes the core of MARS.

In order to work, MARS requires mechanisms for each agent to form expectations of what other agents do in the future. n-th order rationality is one such mechanism. An n-th order rational agent (NORA) assumes that other agents in $\mathbf{\Psi}$ are $(n-1)$-th order rational and best responds to them. A zeroth-order rational agent acts according to a non-strategic heuristic such as randomly drawing strategy from

the HBL or continuing the current strategy. A first-order rational agent assumes that all other agents in $\mathbf{\Psi}$ are zeroth-order rational and best responds to them. A second-order rational agent assumes that all other agents in $\mathbf{\Psi}$ are first-order rational and best responds to them. Observe that if the assumption of a second-order rational agent about other agents in $\mathbf{\Psi}$ is correct; they must assume that the second-order rational agent is zeroth-order rational agent instead of a second-order rational agent.

Myopic Strategies

To describe the algorithm that introduces myopic NORA into $\mathbf{\Psi}$, we denote the level of rationality for an NORA with $d = 0, 1, 2, \ldots$. For simplicity, we assume that $\mathbf{\Psi}$ has two agents A^i and A^j. If the superscript is absent, like in A_d, we refer to any of the two agents with level of rationality d. If the subscript is absent, like in A^i, we refer to agent i regardless of his level of rationality. When A^i has level of rationality d, we label it A^i_d; likewise we label the set containing strategies feasible to A^i_d as $\boldsymbol{\ell}^i_d$:

$d = 0$ A zeroth-order rational agent A^i_0 chooses strategies in $\boldsymbol{\ell}^i_0$;

$d = 1$ A first-order rational agent A^i_1 chooses strategies in $\boldsymbol{\ell}^i_1$

and so forth. Per assumptions of n-th order rationality, from the point of view of A^i_d, the other agent A^j is labeled A^j_{d-1}. Now we show how a myopic NORA uses MARS to derive strategies.

First, let's explore the case of A_0. For simplicity, assume that A^i is zeroth-order rational, that is A^i_0. The set $\boldsymbol{\ell}^i_0$ contains *feasible* strategies that are not conditioned on A^i_0's expectations of what A^j will do. Without assuming that A^j optimizes, A^i_0 arrives at $\boldsymbol{\ell}^i_0$ by using non-strategic heuristics like expert advice, drawing strategies from a fixed probability distribution over the strategy space or sampling the HBL. We set the size of the strategy set for A^i_0 as $\kappa + 1 = \|\boldsymbol{\ell}^i_0\|$. For example, in iterated prisoner's dilemma, "tit for tat" is an appropriate heuristic with $\kappa = 0$. For ease of notation, we say that using non-strategic heuristics is equivalent to launching NORA for $d = 0$:

$$\left\|\boldsymbol{\ell}^i_0\right\| = \text{NORA}\left(A^i_0\right).$$

After A^i_0 computes the set $\boldsymbol{\ell}^i_0$ of feasible strategies, it adopts one strategy in $\boldsymbol{\ell}^i_0$ randomly.

Now let's proceed to the case of A_1. Assume that A^i is first-order rational, that is A^i_1. Recall that A^i_1 assumes that A^j is zeroth-order rational, that is, A^j_0, and forms $\boldsymbol{\ell}^i_1$ by best responding to $\boldsymbol{\ell}^j_0$. If A^i's assumption is true, A^j does not assign a level of rationality to A^i. So A^i_1 finds a strategy that *on average* performs

best when A_0^j adopts any strategy in $\boldsymbol{\ell}_0^j$, integrating out the stochasticity of $\boldsymbol{\Psi}$ by taking K samples for each combination of his candidate strategies and anticipated A_0^j strategies. Algorithm 1 shows this process.

Input: Parameters K, τ, κ and $\boldsymbol{\Psi}$
Output: Set $\boldsymbol{\ell}_1^i$ of feasible strategies for A_1^i
Compute set $\boldsymbol{\ell}_0^{-i} = \text{NORA}\left(A_0^{-i}\right)$;
foreach *strategy* a_1 *available to* A^i **do**
  Initialize strategy payoff $\bar{p}\left(a_1\right) = 0$;
  foreach $a_0 \in \boldsymbol{\ell}_0^{-i}$ **do**
    foreach $k \leqslant K$ **do**
      $s =$ cloned $\boldsymbol{\Psi}$;
      Set strategies a_1, a_0 for both agents and run $\boldsymbol{\Psi}$;
      Query simulation for A^i's payoff and add it to $\bar{p}\left(a_1\right)$;
    end
  end
  Compute average strategy payoff $\bar{p}\left(a_1\right)$ over all samples taken;
end
Eliminate all but τ top strategies for A^i;
Compute the set $\boldsymbol{\ell}_0^i = \text{NORA}\left(A_0^i\right)$;
Add both sets arriving at $\boldsymbol{\ell}_1^i$;

Algorithm 1: Algorithm NORA $\left(A_1^i\right)$.

Best response formation for A_2 follows in a similar vein. Again, assume A_2^i. This assumptions means that A_2^i best responds to A_1^j. Therefore, A_2^i assumes that A_1^j *assumes* that the A_2^i is indeed A_0^i. A_2^i finds a strategy that *on average* performs best when A_1^j adopts *any* strategy in $\boldsymbol{\ell}_1^j$. In order to accomplish this, A_2^i puts himself in his opponent's mind by assuming that it is A_0^i, instead of A_2^i; computes $\boldsymbol{\ell}_1^j$ for A_1^j, and then best responds to the $\boldsymbol{\ell}_1^j$ it has computed. The scheme repeats for any $d > 1$. Note that the size of $\boldsymbol{\ell}_0$ for any A_0 is $1 + \kappa$. For any $A_{d>0}$, the size of $\boldsymbol{\ell}_d$ is $\tau + \kappa$.

Summary

NORA fully decouples the environment from behavior representation, thus injecting strategic reasoning into any multiagent simulation, the most general paradigm to model complex system to date (Axtell 2000). Curiously, it achieves this goal by bringing n-th order rationality and recursive simulation together. Gilmer (2003) and Gilmer and Sullivan (2005) used recursive simulation to help decision making

and Durfee and Vidal (2003; 1995), Hu and Weliman (2001), and Gmytrasiewicz et al. (1998) implemented n-th order rationality in multiagent models, but to the best of our knowledge, we combined the two techniques for the first time.

NORA derives optimum strategies for an agent by computing *average* payoffs for its opponent that hedge against *both* model stochasticity and agents' coevolving strategies by varying $K > 0$ and $\tau > 0$. K determines the number of times a pair of strategies are played against one another, therefore higher K reduces the effects of model randomness on choosing strategies. τ shows the number of equally good strategies an agent is willing to grant its opponent. Depending on the level of risk an agent is willing to accept, the difference among these averages may turn out to be significant or not. Running sensitivity analyses on K and τ or adopting other robustness criteria such as minimax, maximin or Hurwicz measures (Rosenhead et al. 1972) enables decision makers to choose strategies with a desired level of robustness with respect to the environment and opponent and informs them about how much efficiency they trade for any level of desired robustness. NORA also fuses strategic decision making with fictitious best response. $\kappa \geqslant 0$ represents the number of samples an agent wishes to draw from history, so the higher the opponent's κ is, the closer an agent is to playing fictitious best response.[2]

References

Axtell, R. (2000). Why Agents? On the Varied Motivations for Agent Computing in the Social Sciences. Technical Report 17, Center on Social Dynamics, The Brookings Institution.

Brown, G., Carlyle, M., and Wood, K. (2008). *Bioterrorist Risk Assessment: A Call for Change*, chapter Optimizing Department of Homeland Security Defense Investments: Applying Defender-Attacker (-Defender) Optimization To Terror Risk Assessment and Mitigation, pages 90–102. National Academies Press.

Crawford, V. and Haller, H. (1990). Learning How to Cooperate: Optimal Play in Repeated Coordination Games. *Econometrica*, 58(3):571–595.

Daskalakis, C., Goldberg, D., and Papadimitriou, C. (2006). The Complexity of Computing a Nash Equilibrium. *Proceedings of the Thirty-eighth Annual ACM Symposium on Theory of Computing*, pages 71–78.

[2]The computational implementation of myopic and replanning NORA, called RENORA, along with additional papers can be downloaded from the following public repository `https://www.assembla.com/wiki/show/recursiveengines`

Durfee, E. H. and Vidal, J. M. (1995). Recursive Agent Modeling Using Limited Rationality. *Proceedings of the First International Conference on Multi-Agent Systems*, pages 125–132.

Durfee, E. H. and Vidal, J. M. (2003). Predicting the Expected Behavior of Agents That Learn About Agents: The CLRI Framework. *Autonomous Agents and Multiagent Systems*, 6(1):77–107.

Fishman, B. (2009). Dysfunction and Decline: Lessons Learned from Inside Al-Qa'ida in Iraq. Technical report, Center for Combating Terrorism, West Point Military Academy.

Gilmer, J. (2003). The Use of Recursive Simulation to Support Decisionmaking. In Chick, S., Sanchez, P. J., Ferrin, D., and Morrice, D., editors, *Proceedings of the 2003 Winter Simulation Conference*, pages 1116–1112.

Gilmer, J. B. and Sullivan, F. (2005). Issues in Event Analysis for Recursive Simulation. *Proceedings of the 37th Winter Simulation Conference*, pages 12–41.

Gmytrasiewicz, P., Noh, S., and Kellogg, T. (1998). Bayesian Update of Recursive Agent Models. *User Modeling and User-Adapted Interaction*, 8:49–69.

Hao, M., Jin, S., and Zhuang, J. (2009). Robustness of Optimal Defensive Resource Allocations in the Face of Less Fully Rational Attacker. In *Proceedings of the 2009 Industrial Engineering Research Conference*, pages 886–891.

Heuer, R. (1981). Strategic Deception and Counterdeception: A Cognitive Process Approach. *International Studies Quarterly*, 25(2):294–327.

Hu, J. and Weliman, M. P. (2001). Learning about Other Agents in a Dynamic Multiagent System. *Cognitive Systems Research*, 2:67–79.

Jackson, B. and Frelinger, D. (2009). *Understanding Why Terrorist Operations Succeed or Fail*. Rand Homeland Security Program.

Jenelius, E. and Holmgren, J. (2009). Critical Infrastructure Protection Under Imperfect Attacker Perception. *International Journal of Critical Infrastructure Protection*, 3:5–25.

McLean, C., Jain, S., and Lee, Y. (2008). Homeland Security Simulation Domain: A Needs Analysis Overview. *Simulation*.

Parunak, H., Belding, T., Bisson, R., Brueckner, S., Downs, E., Hilscher, R., and Decker, K. (2009). Stigmergic Modeling of Hierarchical Task Networks. In *Proceedings of the Tenth International Workshop on Multi-Agent-Based Simulation*.

Powell, R. (2007). Allocating Defensive Resources with Private Information about Vulnerability. *American Political Science Review*, 101(4):799–809.

Powell, R. (2008). Deterring and Defending Against Strategic Attackers: Deciding How Much to Spend and on What. Technical Report April, Travers Department of Political Science, University of California Berkley.

Rao, A. S. and Georgeff, M. P. (1991). Modeling Rational Agents within a BDI-Architecture. In Allen, J., Fikes, R., and Sandewall, E., editors, *Proceedings of the 2nd International Conference on Principles of Knowledge Representation and Reasoning*, pages 473–484. Morgan Kaufmann Publishers Inc.: San Mateo, CA.

Rosenhead, J., Elton, M., and Gupta, S. (1972). Robustness and Optimality as Criteria for Strategic Decisions. *Operational Research Quarterly*, 23(4):413–431.

Sandler, T. and Siqueira, K. (2008). Games and Terrorism: Recent Developments. *Simulation and Gaming*, 40(2):164–192.

Schreiber, C., Singh, S., and Carley, K. (2004). CONSTRUCT: A Multi-agent Network Model for the Coevolution of Agents and Socio-cultural Environments. Technical Report CMU-ISRI-07, Institute for Software Research, Carnegie Mellon University.

Tate, A. (1977). Generating Project Networks. In *Proceedings of the 5th International Joint Conference on Artificial Intelligence*, pages 888–893.

Taylor, M. P. and Allen, H. (1992). The Use of Technical Analysis in the Foreign Exchange Market. *Journal of International Money and Finance*, 11:304–314.

Tsai, J., Rathi, S., Kiekintveld, C., Ordóñez, F., and Tambe, M. (2008). IRIS-A Tool for Strategic Security Allocation in Transportation Networks. In *Proceedings of the Industry Track of the Eighth International Joint Conference on Autonomous Agents and Multi-agent Systems*, pages 37–44.

Tsai, J., Yin, Z., Kwak, J., Kempe, D., Kiekintveld, C., and Tambe, M. (2009). Strategic Security Placement in Network Domains with Applications to Transit Security. In *Proceedings of IJCAI 2009 Workshop on Quantitative Risk Analysis for Security Applications*.

Tsvetovat, M. and Łatek, M. (2009). Dynamics of Agent Organizations: Application to Modeling Irregular Warfare. *Multi-Agent-Based Simulation*, pages 60–70.

Zhuang, J., Bier, V. M., and Alagoz, O. (2010). Modeling Secrecy and Deception in a Multiple-period Attacker-Defender Signaling Game. *European Journal of Operational Research*, 203(2):409–418.

Copyright of Journal of Homeland Security & Emergency Management is the property of Berkeley Electronic Press and its content may not be copied or emailed to multiple sites or posted to a listserv without the copyright holder's express written permission. However, users may print, download, or email articles for individual use.