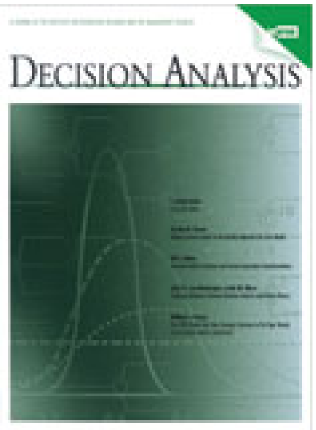


Decision Analysis

Publication details, including instructions for authors and subscription information:
http://pubsonline.informs.org

Games, Risks, and Analytics: Several Illustrative Cases Involving National Security and Management Situations

M. Elisabeth Paté-Cornell,

DECISION ANALYSIS
Vol. 9, No. 2, June 2012, pp. 186–203
ISSN 1545-8490 (print) | ISSN 1545-8504 (online)

http://dx.doi.org/10.1287/deca.1120.0241

Games, Risks, and Analytics: Several Illustrative Cases Involving National Security and Management Situations

M. Elisabeth Paté-Cornell
Department of Management Science and Engineering, Stanford University, Stanford, California 94305, mep@stanford.edu

This paper presents and compares four models of games and risk analyses designed to support strategic and policy decisions, three focusing on national security issues and one on project management. They share a common core of probability, linked decisions among the parties involved, and risks to a principal decision maker. Their structure is based on systems and decision analysis. Their level of complexity depends on the strategies, the environment, and assumptions of variation over time of probabilities, preferences, and options. They are part of the field of analytics and some of its real-life applications. The first model is based on a one-move game, in which the United States faces risks of terrorist attacks by several possible groups using various types of weapons. The result is a probabilistic ranking, at a given time, of the threat posed by these weapons. The second model is a dynamic simulation of counterterrorism scenarios in an alternate game between a government and a terrorist group. The objective is to compare the stabilizing effects of different short- and long-term government strategies. The third model is a dynamic evaluation of nuclear counterproliferation strategies involving an analysis of the weapon development program of a particular country with evolving intent and capabilities and of the effectiveness of different U.S. strategies to prevent or delay its success. The fourth model is a principal–agent representation of the development of an engineered system, in which an agent in charge of part of the project may consider meeting a deadline by cutting corners if he falls behind schedule, generally increasing the system failure probability. The goal is to support the decisions of the manager in setting constraints and incentives. This paper shows how a set of similar game and risk analysis models at different levels of complexity can provide valuable insights to decision makers, both in national security and management situations, and help them avoid mistakes such as excessive focus on the short term and underestimation of dependencies. It compares their capabilities, including the number of moves, dynamics of the underlying situation, possible changes of context, actors' preferences and strategic options, and risk characterization.

Key words: game analysis; risk analysis; analytics; national security; failure probability; counterterrorism; nuclear proliferation; principal–agent model; practice
History: Received on August 12, 2011. Accepted on March 1, 2012, after 1 revision.

1. Games Involving People (vs. Nature): Four Cases

1.1. Games Against Adversaries or, Simply, Agents

Consider the problem faced by the U.S. government when trying to allocate its resources—protection, intelligence, research—against various types of possible weapons in the hands of different terrorist groups. Some, such as a nuclear warhead, can cause immense damage to the United States but are less attractive to opportunistic attackers than are conventional explosives and are thus a less likely threat. A biological attack is another possibility that requires different types of detection and protection investments.[1] Consider next the case of a government facing an insurgency and determined to address, through its investments, both the immediate risk mitigation problems and the roots of the insurrection.[2] The objective is to reach a certain level of stability in a given time frame, and discounting is critical to an analysis of investment decisions. Examine, then, the consequences of different U.S. strategies to prevent or slow

[1] One challenge with a biological attack is to detect the signals and distinguish it from a natural occurrence.

[2] This is presumably the case of the Afghan government with the support of U.S. forces in the last few years.

down the development of nuclear weapons by a specific country such as Iran or North Korea, a problem currently faced by the United States and its allies. The question is how to delay, prevent, or limit the program completion. Consider finally what looks like a different problem but is in fact similar in structure: a project management situation in which a principal tries to reduce the risks of a system's failure by influencing the behavior of an agent working under time constraints. These four problems have a common core: they involve one or more decisions under uncertainty about the other side(s)' behavior(s); external factors (international situation, the system's robustness, etc.); and the risks of failure of the chosen strategy.

1.2. Decisions Analysis for Both Sides: The Dynamics of Alternate Games

Decision analysis (e.g., Raiffa 1968, Howard 1968) is used here from the perspective of a principal decision maker in a game situation. The other side's behavior may be described by different types of models such as bounded rationality. The residual risk to the decision maker can be represented, for instance, by a failure probability or by the probability distribution of negative outcomes (e.g., the time to completion of a nuclear weapons program by an adversary).

Rational decision models (von Neumann and Morgenstern 1947) were used initially in game theory, with or without characterization of uncertainties, to represent moves by two or more parties and generally to find a Nash equilibrium (Harsanyi 1959, Gibbons 1992). In some cases, however, the decision makers and their preferences do change over time, and each side may be uncertain about the preferences and/or the state of information of the other(s). Decision analysis can then be used in a game analysis from the point of view of the main decision maker to include relevant and variable parameters, and if needed, the rationality assumption of the adversary (or agent) can be modified to represent other behaviors.

1.3. What Are the Risks of Different Strategies to the Main Decision Maker?

This paper presents several examples of assessment of the risks involved in such games and shows the fit between different models and the decision support needed to set priorities. Four models are presented here as cases of games and risk analyses with different structures, dynamics, levels of complexity, and types of situations.[3] The objective of this paper is to examine their evolution and to compare their capabilities. Because relevant statistics generally do not exist for these kinds of situations, they are based mostly on Bayesian probability (e.g., de Finetti 1970) and on systems analysis extended to group behaviors.

1.4. Four Decision Support Models Involving Security or Management

Developed in the wake of the 9/11 attacks on U.S. territory, the first model was developed to assess the probabilities of the use of different types of weapons in terrorist attacks. It represents a one-move game involving several possible adversaries (Paté-Cornell and Guikema 2002). It is based on bounded rationality and yields the risks (probabilities and consequences) to the United States of different types of hostile actions and a probability-based ranking of different weapons' threats. It provides information for defensive resources' allocation.

The second model, a counterinsurgency analysis framework, is designed to support a government's investment decisions against one insurgent group. It is a simulation of an alternative repeated game in which both parties are assumed to act rationally but have incomplete information about the other's last move (Kucik 2007, Paté-Cornell and Kucik 2012). The illustration is the case of a village in the Philippines between 2000 and 2003. The risk result is the probability that, in the end of the chosen period, the stability of the region is below a certain level.

The third model is a nuclear counterproliferation strategic analysis, based on dynamic programming, designed to support U.S. strategies to prevent or slow down the development of nuclear weapons by a specified country (Caswell 2010, Caswell et al. 2011, Caswell and Paté-Cornell 2011). Perceptions and strategies are allowed to vary with the country's progress and intent under international and domestic influences. The model involves a two-tier Bayesian

[3] These four models represent studies performed at Stanford University in the Engineering Risk Research Group of the Department of Management Science and Engineering (from 2001 to 2011) Three of these models have been described in Paté-Cornell et al. (2008).

network representing U.S. uncertainties about the country's intent and capabilities and a long-term optimization to identify the best U.S. strategy over time, with illustration by the retrospective cases of South Africa and Pakistan and the ongoing case of Iran.

The fourth model is similar in its structure but shows an application to a management situation. It is a principal–agent model designed to support the management of an engineered system's development under constraints. A manager sets incentives and monitoring levels for an agent to perform a task on time. The agent, if he falls behind, may consider taking shortcuts, thus increasing the risks of the system's failure (Garber 2007, Garber and Paté-Cornell 2011). Both sides are assumed to be rational but not to have full information about the actions of the other. To show the possible increase in the system's failure risks given the agent's effort level and his shortcut decision if he falls behind, the model includes a probabilistic risk analysis of the system's performance. The goal is to support the principal's decisions about incentives and constraints. Therefore, this kind of analysis also permits assessing the shadow price of the schedule constraint.

These four models and their applications clearly represent a small sample of the literature that has been published on game theory and risk analysis (e.g., Bier and Azaiez 2008), including dynamic programming (e.g., Bellman 1957, Bertsekas 2000) and stochastic games (e.g., Shoham and Leyton-Brown 2009). They are generally based on assumptions of actors' rationality or bounded rationality.[4] In the field of counterterrorism in particular, there has been a substantial body of work, for example, by Cox (2009) on attacker–defender models; by Feng and Keller (2006), Willis (2007), Bier (2007), Bier and von Winterfeldt (2007), and Dillon et al. (2009) on setting priorities among protective measures; by Parnell et al. (2010) on game/risk modeling of bioterrorism risk management; and by Merrick and Parnell (2011) and Lloyd and Merrick (2011) on applications of risk and decision analysis to counterterrorism problems. This paper shows that similar frameworks can be applied to a spectrum of adversarial situations, including open conflicts, or simply to related decisions by two parties with different interests. These types of models have application to many fields, including engineering management, business competition, legal disputes, or medical decisions. What follows includes a brief description of each model and a discussion of their relative capabilities.

2. A One-Move Game for the Ranking of Different Types of Terrorist Attacks on the United States[5]

2.1. The Problem of Allocating Counterterrorism Resources

In 2001, the terrorist attacks on the United States alerted the country that defenses had to be put in place and that responses to different types of terrorist attacks (and weapons) had to be planned. Given resource limitations, priorities had to be set. The main question was to assess the probabilities of different types of attacks on U.S. soil based mostly on intelligence information. The intent was to focus on four general types of weapons: biological, "dirty bombs," repeated conventional attacks in urban environments, and explosion of a nuclear warhead. The objective was to compare the probabilities of these four classes of scenarios to support an efficient allocation of defense resources. A Bayesian network was constructed, using illustrative but credible data, to compute the probabilities of different attack types.

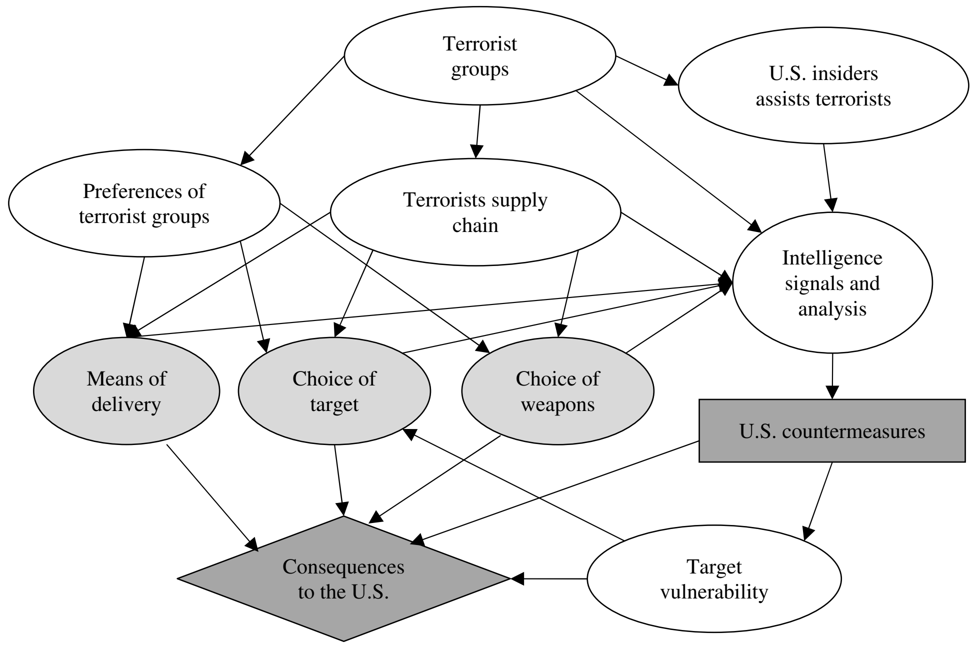
2.2. The State Variables of the U.S. Decision Model

Figure 1 represents a Bayesian network or influence diagram (Paté-Cornell and Guikema 2002), involving decisions, states, and consequences nodes. "Terrorist groups" include both extremist Islamists and disgruntled American groups (e.g., white supremacists) and probabilities that at a given time, each is planning some kind of attack. Attack scenarios involve three elements: the choice of weapons, the choice of a target, and the means of delivery. In the chosen illustration, the targets are cities and gathering sites, civilian

[4] An assumption of rationality allows formulating closed-form solutions. Other behavioral models can be used, but they would generally require simulation to obtain a final result.

[5] With the collaboration of Seth Guikema (Johns Hopkins University, Baltimore, Maryland 21218). Parts of this section are taken from Paté-Cornell and Guikema (2002).

Figure 1 **Influence Diagram Yielding the Risks of Different Attack Scenarios on the United States from Several Possible Terrorist Groups**



Source. Paté-Cornell and Guikema (2002).

or military infrastructure and equipment, symbolic structures and embassies, aircraft and other means of transportation, and nuclear power plants. The means of delivery include trucks and cars, airplanes, ships, or people (e.g., suicide bombers).

These choices are based in part on terrorist groups' objectives (to the best of our knowledge). These are represented by multiattribute utility functions reflecting their preferences for different types of impacts including the number of casualties, economic damage, instability, loss of liberties, restriction of movement, loss of international influence and prestige, and leadership of the country attacked. Some of the attack effects can be directly computed (e.g., probability distribution for the number of casualties); others have to be described by a carefully designed index (e.g., the loss of prestige). Knowledge of attackers' preferences can be based on many sources including their own statements and intelligence information[6] as well as open sources such as speeches or reporting in the local press.

Five elements at the disposal of each group constitute its "supply chain" and are considered critical to the feasibility of a given type of attack: the people willing to participate and their level of skills, communications, transportation, cash, and available equipment and weapons.[7] One critical factor to penetrating a protected target is then the potential of insiders' help, e.g., the complicity of airline or airport personnel, military personnel, harbor operators, etc.

The U.S. assessment of the chances of each of these scenarios depends on the quality and analysis of intelligence—unexpected tips as well as systematically collected signals—which must be updated in real time to account for new information and conditions. These include the outcomes of previous operations and the

[6] After the 9/11 attacks, Al Qaeda's documents showed its reluctance to attack nuclear power plants. Later, its leadership stated that killing a maximum number of Americans and their allies may not be in its best interest.

[7] Communications, for example, were critical at the beginning of the fight against Al Qaeda, when they involved cell phones and electronic transmissions. In the end, it was the necessary use of human couriers that led to the targeting and killing of Osama Bin Laden in May 2011. Cash is also critical: mounting an attack may not necessarily require large sums but payment of people requires some transfers of money. Transportation, people, and weapons may thus be at this time the most observable elements of terrorist capabilities.

location of new sources of materials and also organizational changes such as new leadership, internal rivalries, political changes such as a shift in alliance, and a technological shift such as a breakthrough in nuclear weapons acquisition. The dynamics of intelligence gathering, analysis, and communication to decision makers is thus critical to the timeliness of countermeasures including reduction of threats and vulnerabilities. The first objective is to stop a plot by arresting or eliminating the perpetrators and the second to mitigate an attack's effects by protecting structures, decreasing access, and mitigating damage.

The resulting risk to the United States is represented by the diamond at the bottom of Figure 1. It is the joint distribution of the potential damage inflicted on the United States by terrorists using different kinds of weapons. One key assumption here, which differs from classical game theory, is that the probability of different attack scenarios is proportional to their expected utility to the terrorist groups as assessed by U.S. intelligence. This model, based on notions of bounded rationality (e.g., Simon 1957, Kahneman 2003), is one of Luce's choice models (Luce 1977).

The characteristics of this model are thus a single move, two adversaries, an assumption of bounded rationality, and the use of a Bayesian network. The ranking of the threats of different types of weapons based on their probability of use by terrorists was found to be nuclear warheads, biological attacks, repeated urban conventional attacks, and dirty bombs. This study was one of the first of that kind following the 9/11 attacks on the United States, encompassing in a relatively simple model the main elements of an optimal allocation of defense resources (as opposed to a uniform spread).

3. Simulation of a Repeated Game: Application to Counterinsurgency[8]

3.1. The Counterinsurgency Model

This model is based on an analysis of moves and countermoves by two parties, in this case a government whose goal is to stabilize the country and insurgents who want to seize power. It is designed to support the decisions of a government, which at each time unit of a specified horizon allocates funds to counter the insurgency, some to repel immediate attacks and some longer-term investments to address the social problems that fuel the conflict—infrastructure, medical needs, or education (Kucik 2007). The model carries over each cash flow for the rest of its time horizon. The discount rate is thus a key factor.[9] Two intertwined influence diagrams represent the alternate moves of both parties (Figure 2).

This model is thus a version of an attacker–defender game between two actors with valuation functions that depend on the (uncertain) system state (e.g., political and economic situation). Moves and countermoves are repeated in a simulation. Both sides' preferences are represented by linear multiattribute utility functions.[10] The insurgents' state of information and utility are assessed by the government based on available intelligence. Each side's move affects the population and determines the situation in which the other side makes its next move.

The attributes of the government's utility function are the population's economic situation;[11] political, social, and religious situation;[12] the security level;[13] the initiative of combat operations;[14] and their counterinsurgency precision.[15] The country's stability attribute is used to measure the effectiveness (and the risk of failure) of a government's policy. The strategic options of the insurgents are to launch an attack, organize civil disobedience, or seek a lasting peace. Their

[8] With the collaboration of Paul Kucik (U.S. Military Academy, West Point, New York 10996). Parts of this section are taken from Kucik and Paté-Cornell (2012).

[9] This discount rate includes both the economic rate of the government, e.g., its borrowing rate, and its political time preference given its leadership's perception of the urgency of the situation.

[10] This form assumes utility independence. If that assumption does not hold, cross-terms can be introduced.

[11] Measured by the percentage of the people who live below the poverty line.

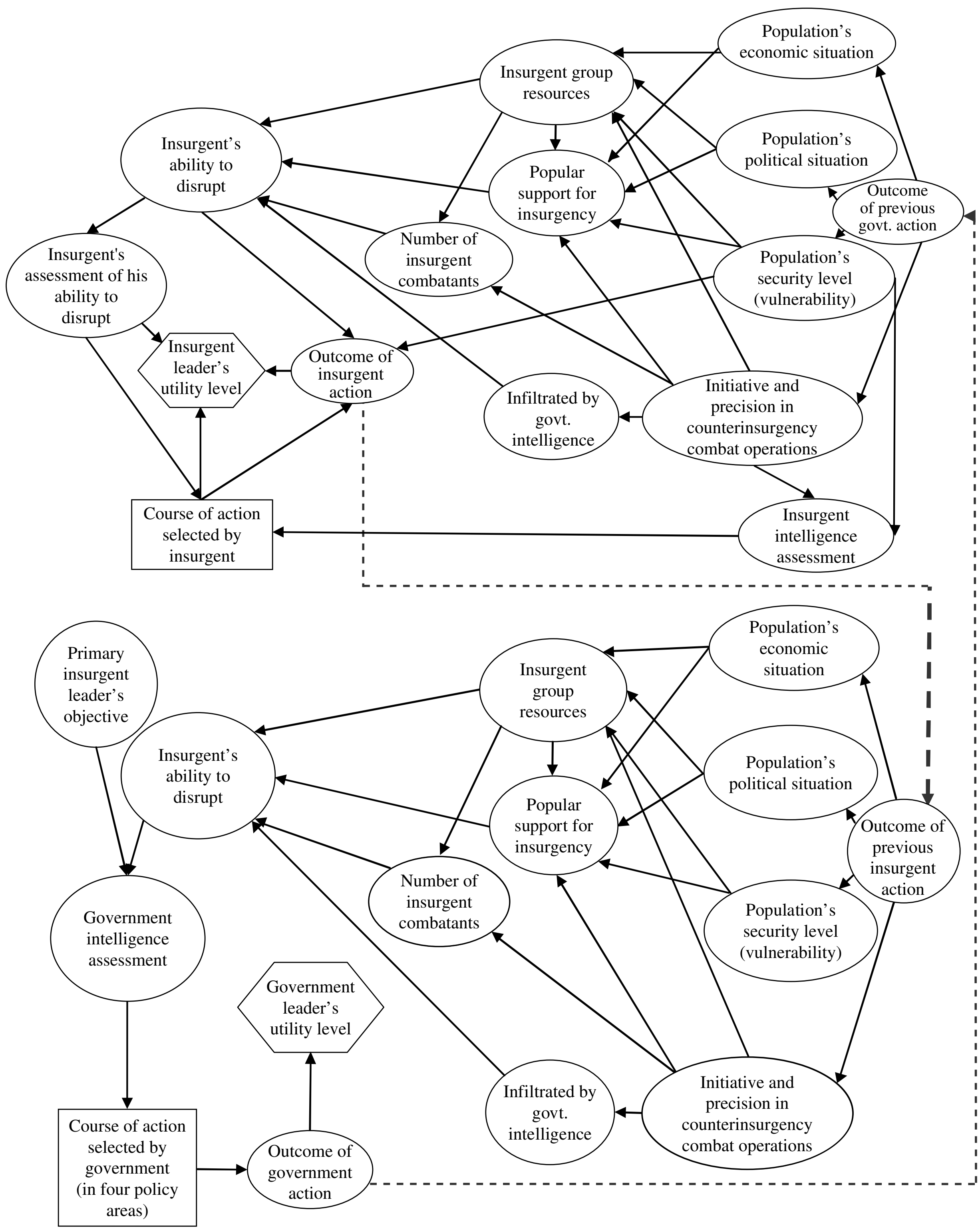
[12] Measured by the percentage of the people dissatisfied with noneconomic conditions such as the relative balance of power of different groups, e.g., different religious factions.

[13] Measured by the number of actionable human intelligence tips received by the government in the past n time units (here, three months) divided by the number of insurgent attack initiatives.

[14] Measured by the fraction of combat engagements initiated by the government forces.

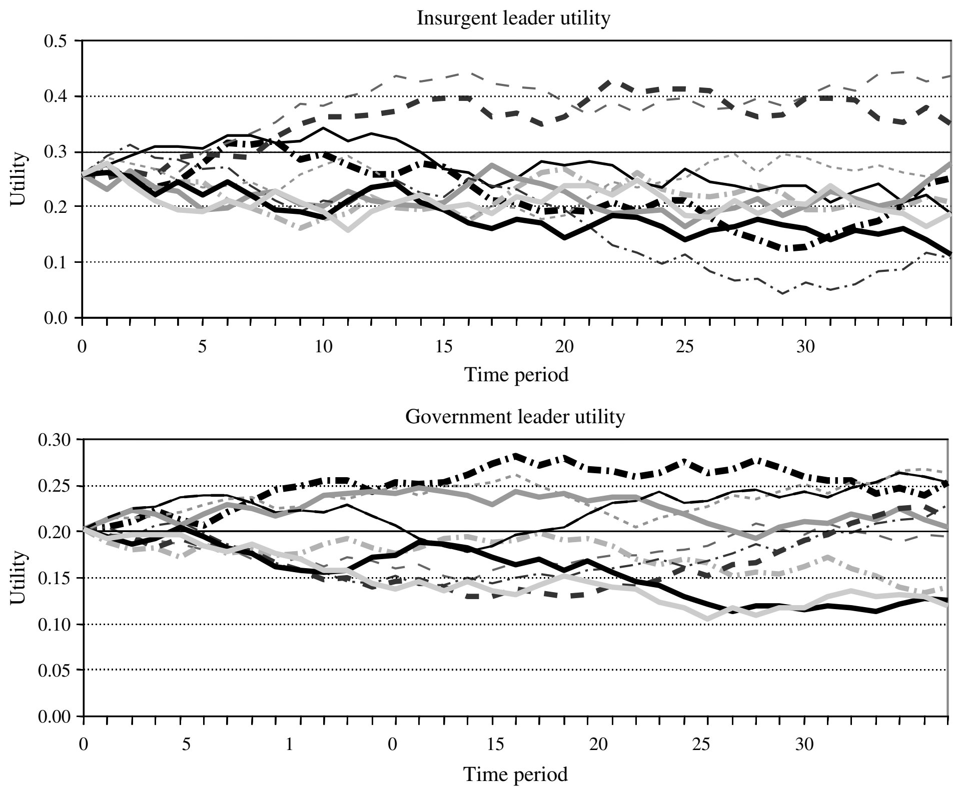
[15] Measured by the fraction of people killed by government forces who are actually insurgents.

Figure 2 **Linked Influence Diagrams Representing Alternate Moves of a Government and a Group of Insurgents**



Source. Kucik (2007), Kucik and Paté-Cornell (2012).

Figure 3 **Results of the Dynamic Simulation of the Game Between Government and Insurgent in the Philippine Illustration**



Source. Kucik (2007), Kucik and Paté-Cornell (2012).

multiattribute utility function is similar to that of the government. Both are linear combinations of factors measuring their preferences. At each step, each side observes the other's past move, assesses the probabilities of different current situations, and makes its next decision based on its preferences and discount rate at that time. As shown in Figure 2, the link between the two influence diagrams is that the outcome of each side's action is the starting point of the other's decision.

The resulting probability of meeting an economic or political stability threshold allows assessing the success of the considered strategy and comparing short-term and long-term investments in immediate security versus nation building measures. This information may help leaders understand the underlying dynamics of a situation and provides a balance to natural inclinations to focus on the short term.

3.2. The Philippine Illustration

This model was applied retroactively to the case of an insurgency in a village of the Philippines over three years[16] (2000–2003), based on actual Philippine government data. Figure 3 shows the results of that simulation as a sample of simulation paths for the Country Stability attribute. At the starting time, that stability level had a value of 0.203 on a scale of 0 to 1. The end point distribution of that attribute showed the dispersion of the various scenarios' results over time, with a 5th percentile of 0.171, a median of 0.206, and a 95th percentile of 0.234. In other terms, the model did not anticipate a high probability of significant improvement for the policy that was actually implemented. Comparing these results with the events that actually unfolded showed that the state of the village in 2003 turned out to be roughly the median of the results of the simulated game.

The challenges of this model were to identify the government's options, to assess the parameters of both sides' decisions, and to choose a useful form

[16] The simulation was performed as if only the starting point were known.

of results. The dynamic aspect of the policy analysis, the discounting factor involved, and the simulation model that was adopted made it a clear evolution of the previous model, which was static in nature.

4. Nuclear Counterproliferation Strategies: Dynamic Model in an Evolving Environment[17]

4.1. The Strategic Decision Framework

This more complex model represents a long-term repeated game between a country determined to develop a nuclear capability (e.g., Iran or North Korea) and a government (the United States) trying to prevent or slow down this nuclear weapons acquisition (Caswell 2010). The objective is to support U.S. counternuclear proliferation strategies, given uncertainties and changes in the country's intent and capabilities as well as in the world environment. It is a dynamic programming model whose objective is to determine, at any given time, the optimal U.S. strategy and the corresponding mean time to the country's nuclear weapons' acquisition.

The United States, at each step, assesses the intent and capability of the considered country toward nuclear weapons and choose its best long-term counterproliferation strategy involving three types of actions: diplomatic, military, and economic. These decisions are made considering that the world's environment is likely to evolve over the considered time horizon. Therefore, the two main dynamic components of the model are the country's development of nuclear weapons (and the uncertainties attached to them from the U.S. perspective) and a U.S. strategy that can vary over time given the uncertainty of the world's situation and the country's decisions.

The model itself is composed of three modules. First, the proliferating country's decision is described by a Bayesian network, considering its objectives—security, international prestige, domestic politics, and costs—as well as its capabilities, both internally developed and externally acquired (bought or stolen). The second module represents the U.S. perception of this country's intent and capability over a given time horizon. The third module is a decision model designed to support a U.S. strategic decision, considering all options over time given external world events. This model thus involves two main dynamic components: the country's development of nuclear weapons, represented by a Markov decision process, and the analysis of different U.S. counterproliferation strategies, which are allowed to vary over time. Both are based on an assumption of rational choices. The U.S. alternatives at each time are described by combinations of diplomatic, economic, and military options. Given the combinatorial nature of this problem, a genetic algorithm was used in the end to optimize the U.S. strategy. Figure 4 summarizes the structure of the overall strategic analysis model (the three embedded modules are described further).

4.2. The Country's Nuclear Weapon Development Model

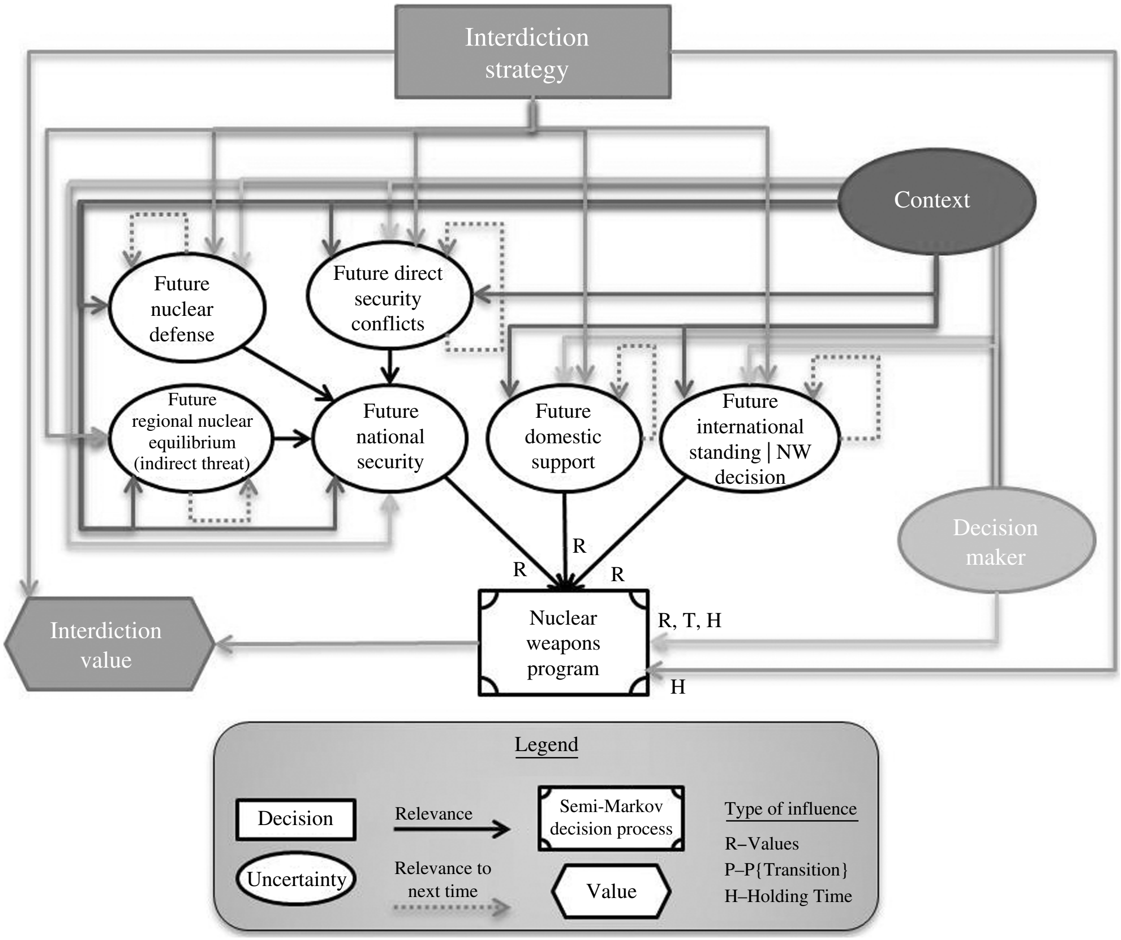
In addition to technical and scientific challenges, the country's decision to develop nuclear weapons is influenced by international norms, domestic politics, and national security concerns (Sagan 1996–1997). It was modeled using a semi-Markov decision process, which implies that the country's decision is based on the world situation and its prospects at each decision time but involves no memory. The alternatives for the country at each point in time are "No Nuclear Weapons;" "Hedge Nuclear Weapons" (actively develop the material, technology, and knowledge needed to develop quickly a latent nuclear weapons capability); or "Possess Nuclear Weapons." At each stage, the country's nuclear capabilities can thus be characterized as one of four states: "Nuclear Weapons Free," "Latent Nuclear Weapons" (everything but the bomb), "Infancy" (a few bombs), or an "Arsenal" (several bombs). The transitions among these states result from sequential decisions of the country's leaders, who consider at each step with different weights and degrees of uncertainty, their security as well as the international and domestic effects of their options.

4.3. The U.S. Strategic Decisions

The next problem is to represent the U.S. perception and understanding of the country's dynamics.

[17] With the collaboration of David Caswell (7th Air Force, Osan, South Korea). Parts of this section are taken from Caswell and Paté-Cornell (2011) and Caswell et al. (2011).

Figure 4 Decision Diagram Representing the Overall Structure of a Nuclear Weapons Program and Counterproliferation Strategy Model for the United States

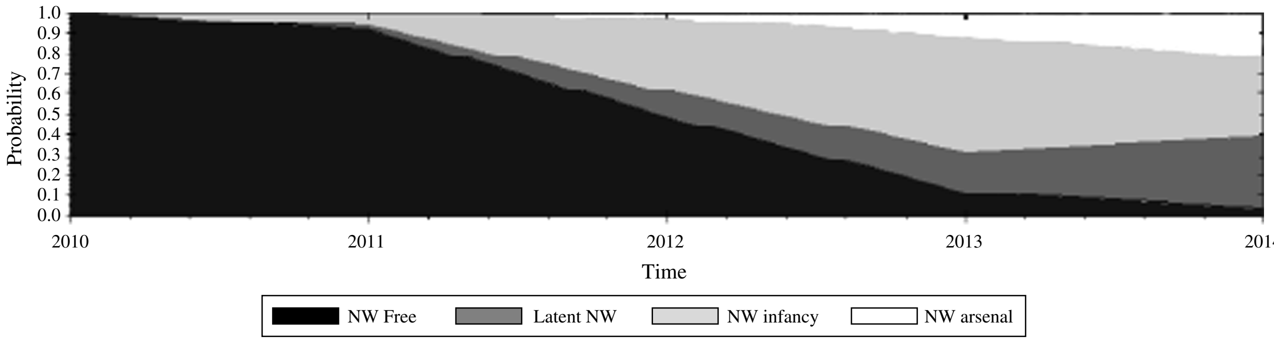


Source. Caswell (2010), Caswell et al. (2011).

The U.S. analysts do not observe directly the developments that take place. Assuming rationality on the country's side, the model of the U.S. perception of the country's decisions is represented here by a semi-Markov decision process. To represent the world's evolution and context and to simplify the representation, a new semi-Markov node (shown in Figure 4) was introduced in the country's decision diagram. Its objective is to provide a compact form of an N-stage semi-Markov decision process and to introduce its dynamics in a Bayesian network (Caswell and Paté-Cornell 2011).

This network representation of the country's decisions allows the United States to assess the eventual results of a strategy, which can change with circumstances (e.g., new leaders on both sides) and new information. It is used as a basis for U.S. counterproliferation decisions. As mentioned earlier, the model includes three dimensions of U.S. options, each with several possible response levels: diplomatic (no action, reprimand, reward); economic (no action, sanction, stimulus); and military (no action, military defense, threat of force, use of minimal force, and use of significant force). Each strategy presents risk–cost trade-offs. For N time units, the optimization of the initial decision involves a choice among 45^N options and a genetic algorithm was used to make the optimization feasible. The results are represented as an expected time to completion at any given date and as

Figure 5 **Illustration of the Probability of Nuclear Weapons Program States Calculated for Each Year for a Given U.S. Strategy and a Specified Country**



Source. Caswell (2010), Caswell et al. (2011).

the probability over time that the country possesses nuclear weapons (see an example in Figure 5).

4.4. Examples of Application: South Africa, Pakistan, and Iran

This model was applied to the cases of South Africa, Pakistan, and Iran. The South African and Pakistan studies are *post facto* analyses of history, in which the context and change of leadership made the country decide to construct and then give up nuclear weapons. The results included first the effects over time of international pressures (including the evolution of the U.S. counterproliferation strategy) on its nuclear weapons program, in the national and international contexts of the time. They also showed the evolution of the expected time to completion or, in the case of South Africa, the eventual abandonment of the program.

4.5. Key Elements of the Strategic Dynamic Model

One of the key characteristics of this model is that both parties' preferences can evolve over time (in addition to the state of information as in the previous model). It has a dynamic programming structure and uses different optimization tools including a genetic algorithm. The country makes decisions based on its intent and its progress toward its goals. The principal (the United States) observes signals of the country's moves, estimates the long-term state of its nuclear weapon program, and optimizes its own long-term strategy accordingly. This approach is again a development of the previous models. It is more complex in that from the beginning, it allows the U.S. long-term decision to evolve, considering the dynamics of its effects thereafter.

5. Managing the Potential of Shortcuts in the Development of an Engineered System[18]

5.1. A Principal–Agent Approach to the Management of a System's Development

Like the previous models, this one describes a game between two parties and the risks to the main decision maker of the outcomes of that game, combining project management and risk analysis. Yet it is different in that it does not address a national security issue or even a directly adversarial situation. Instead, it involves the interaction between a principal (manager of a system's development) who sets parameters, constraints, and incentives for an agent (in charge of a subsystem) who reacts to them (Garber 2007; Garber and Paté-Cornell 2006, 2011). The model is designed to guide the manager's decision and allows computing the "shadow price" of the resource constraints.[19]

The focus is on the manager's (principal's) decisions and the response of the agent (Gibbons 1992, Milgrom and Roberts 1992, Laffont and Martimort 2001). The manager's objectives are a combination of low failure probability, low cost, and meeting the deadline. The agent is a rational decision maker who faces the deadline (or another resource constraint) and the reward system set by the principal. These

[18] With the collaboration of Russ Garber (San Jose, California 95124). Parts of this section are taken from Garber and Paté-Cornell (2011).

[19] This means the effect of relaxing or tightening the schedule by one unit on the overall system's performance in operations. A key assumption here is that the original constraints do not involve slack that can be eliminated at no cost.

constraints and incentives determine, first, the effort that the rational agent is willing to deploy and thus the probability that he falls behind schedule. If he does, he has a choice: to admit to the principal that he is late and to ask for help (presumably at a penalty cost) or to cut corners to catch up, hoping that it will not be discovered. The risk of failure of the whole system later in operations increases depending on the shortcuts he chooses to take if he does. It is assumed that he uses at that stage a probabilistic risk analysis (Henley and Kumamoto 1992) to identify the set of shortcuts that minimizes the corresponding increase of system failure risk.

The model allows assessing the effects of the time constraint and incentive system on the system's performance. The principal's decisions include whether or not to monitor the development progress and three types of penalty costs to the agent: for being late and admitting so, for being caught cutting corners, and for causing a failure in operations.[20] In reality, the principal should want to make sure that the agent does not take shortcuts. The agent's decisions include his level of effort, and if he falls behind, whether to admit so or to take shortcuts. Therefore, to determine his optimal effort level, the agent needs to decide first what he will do if he is late. It is assumed here that the agent can assess and minimize the probability of system failure given which shortcuts he takes. The result is a failure risk given rational decisions on both sides.

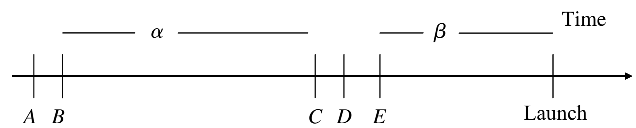
5.2. Model Structure and Illustration

The core of the framework is a principal–agent model of a single move on both sides and a probabilistic risk analysis of the technical system developed by the agent and known to the principal. It is an asymmetric game that assumes rationality on both sides and the principal's knowledge of the agent's utility function. It is also assumed that both parties know the probabilities of component/subsystems failures with and without shortcuts but that the principal does not know whether the project is late and which shortcuts were taken unless he or she monitors progress and discovers them.

Consider the time line shown in Figure 6. At time 0, the principal sets payments, penalties, and inspection

[20] It is assumed that only a fraction of the system failure can be attributed to these shortcuts.

Figure 6 **An Illustrative Timeline for the Principal's and Agent's Decisions**



Source. Garber and Paté-Cornell (2011).

level (A), the agent accepts the project and commits effort resources (B). After α time units (e.g., a critical step in the system's development), the agent discovers whether or not the project is delayed and by how much (C) and decides whether or not to take shortcuts and which ones, depending on how many time units he must regain (D); then the principal inspects the agent's project (E). If shortcuts are detected, the agent is penalized and the system launch is delayed. Finally after β time units, the system is launched, and it is assumed that if it fails, it will be at that time (one can extend the model to consider failure for the operational lifetime of the system).

It is assumed that the agent knows the penalty costs that he could incur and whether or not he is being monitored. The computation algorithm is thus to solve for the agent's decisions and then for the principal's decision (monitoring or trusting the agent, and penalties) and to assess the resulting probability of system failure. The results allow computing of the shadow cost of the schedule constraint by considering the effects of relaxing these constraints on the different parts of the model: the agent's effort level, the probability that he falls behind, his response to being late, and the corresponding variations of the system's failure probability and associated costs.

5.3. A Simple Illustration

This model can be applied to many different cases, e.g., in the building industry.[21] It can also be applied to the risks of skipping tests in the development of a new system, such as a spacecraft, to meet a launch deadline. A simple illustration presented in the original study consisted of a system of three subsystems

[21] For example, in the construction of houses in a seismic area, employees running short of time at the end of a work day may decide to reduce the number of nails in shear walls to meet the deadline, thus increasing the probability of a structural failure in an earthquake.

in a series, two of which are made of one component and the third of two components in parallel. The data included the effect of the deadline on the agent's effort and in turn on the probability that he falls behind schedule, the probabilities of failure (and their dependencies) with and without shortcuts, the time gained by cutting corners in each component (assumed to be additive), the costs of each scenario to both principal and agent, and their utility functions. It turns out that in the chosen illustration, the manager's best option was to not monitor the agent's work and to trust his judgment.[22] In that case, the agent was likely to be late, and if that happened, his best option given the data was a set of shortcuts that minimized the failure risk. In the end, the time constraint had to be relaxed by several units before it made any difference in these decisions and their effect on the system's reliability. In another illustration, using the same system with different numbers, it was shown that the penalties could be set at such a level that the agent would not take shortcuts under any circumstances (Garber and Paté-Cornell 2011).

5.4. Implications of That Model

As is often the case, rather than the numerical results themselves, the main benefit of this model is to provide a way to think about setting appropriate constraints and incentives. In some management decisions that have resulted in an accident, it seemed after the fact that the principal did not want to know the failure risk and set (or accepted) unreasonable deadlines to reduce costs. Therefore, they never considered seriously the effects of the incentives and constraints that they set, the benefits of relaxing them, or the option of reducing the workload if the constraints could not be changed. This model represents an interesting variation of the previous ones in that it addresses a management issue involving a single set of responses to the other side's move and uses a probabilistic risk analysis to assess the increase of the probability of a system's failure influenced by management decisions.

[22] The principal's decision, however, would change if his disutility for lateness decreased and the risk of system failure increased, which would cause his decision to shift to a lower penalty for lateness and a higher one for failure.

6. Lessons Learned from These Models: Achievements and Challenges

6.1. Systems Analysis and Probability in Games and Risk Analyses

These four studies illustrate the powers of analytics in the context of games and risks. They combine probability, systems analysis, games analysis, simulation, optimization, behaviors, reliability, and economics. They are designed to address complex decision support problems when a single analytical tool would not suffice and the information comes from multiple sources. These studies represent a spectrum, and in some aspects a progression, of dynamic game models. All are designed to support the decisions of a principal. Few of their variables can be characterized by classical statistics, either because they do not exist or because the system is in constant flux. Therefore, their distributions rely mostly on Bayesian probabilities. As is often the case, aside from numerical results that vary over time, the main benefits of these models are the insights that they provide based on their structure and logics. They provide a perspective that permits avoiding serious mistakes such as ignoring uncertainties (overconfidence), overemphasizing the most recent piece of information (ignoring the priors), or focusing on the immediate effects of an action without sufficient consideration of delayed consequences.

In all four cases, the problem formulation was the main and first challenge: What are the key hypotheses (e.g., of rationality), what is the best model structure, which variables should be included, what are the dependencies to represent, and what attributes of the outcomes truly matter? How do we represent the game and decisions' dynamics as well as the results in a useful manner? What are the best sources of information and data? And in the end, what has been achieved and what are the remaining challenges?

6.2. The Models' Structures: Analytical Challenges and Choices

These models are part of—and in some cases include—decision analyses. In all cases, their structures were characterized by one or several influence diagrams to display uncertainties, dependencies, and the effects of the principal's decision on the result.

These networks or their subroutines were activated at each time unit to simulate the system's evolution. The model's variables, structure, and dynamics were guided by the form of the desired results: a simple system failure probability and associated costs (project management); a threat ranking based on relative probabilities and effects on the United States (terrorist weapons); failure to achieve a threshold of success in counterterrorism (country stability); or cancellation of a nuclear program or distribution of delays of its success (counterproliferation).

For the ranking of weapon threats, the model structure is comparatively simple because dynamics are not explicitly considered. The result is a relative probability of weapon use and expected damage to the United States at a given time, based on attack scenarios and U.S. disutilities. The first challenge was to identify and select the groups considered. It was clear that domestic groups were to be included along with foreign extremists. The difficulty regarding the latter is that they are multiple and constantly evolving in their structures and their alliances. Two simplifying assumptions were thus made: first, to restrict the number of considered terrorist groups—essentially along the lines of their objectives—and second, to assume that only one group was plotting an attack at a given time. Both assumptions (a small number of groups and a single plot) can easily be relaxed with more powerful computational capabilities to handle large Bayesian networks, to reflect relevant dependencies, and to update regularly the fluctuations of the groups' structures. Another main analytical choice was to focus on the terrorist supply chain and its key components (people, weapons,[23] communications, transportation, and cash),[24] leading to the characterization of attacks by the nature of the target, the weapon, and the means of delivery. What was not considered were scenarios involving simultaneous attacks, which would require further adaptation of the model to include detection of concerted hostile actions.[25] Other dependencies among attacks can occur, for instance, through a "copycat" effect, in which the success of one operation increases the probability that it happens again elsewhere.[26] For each group, modeling this effect would require representation, in their supply chain, of the resources needed to replicate the last attack and of their willingness to do so.

The counterterrorism model was more complex in its formulation because it involved the dynamics of sequential decisions of two actors, and it assumed an alternate game. The main formulation issue was to select the characteristics of the population's situation that most influenced its support of either the government or the insurgents.[27] In that sense, it was a three-actor game reduced to two, where the third party's behavior (the country's inhabitants') was modeled as a state variable. An alternative would be to consider separately the preferences of the population and their evolution as the conflict unfolds as well as the possibility that a new leadership emerges independently of the current government and the main terrorist group. A still more complex formulation would involve several such groups, with changing interactions, alliances, and conflicts among them. In that case, the game would have to be extended to include these interactions, which would require an overarching dynamic model to integrate the different actors' moves and their effects.

[23] A group of students led by Paul Kucik investigated on the Internet the structure and the operation of the AQ Kahn network and its marketing of nuclear enrichment capabilities.

[24] In that part of the work, the author learned from Swiss experts about the transfer of noncash assets in the Middle East at the time.

[25] In reality, exercises such as TOPOFF (Top Official) are conducted regularly at the national level by the Department of Homeland Security and the Office of Domestic Preparedness to recognize and react to simultaneous attacks, for instance a dirty bomb in one place and the release of a deadly bioagent in another. One of the problems in that case was that bioattacks are difficult to detect and to distinguish from natural occurrences.

[26] Clearly, in the United States the risk of an attack using an airline plane as a weapon has increased considerably after 9/11, and massive resources were mobilized against that possibility. One can argue that this attack was not independent of a previous attack on an Air France flight in 1994 when a group of terrorists took over, in Algiers, an aircraft bound to Paris and were stopped on their way and killed in Marseille.

[27] Insurgents' support may be caused by the population's discontent but also by hope for their help in everyday life. One example is that of Hezbollah in Lebanon playing a humanitarian role through the "Hezbollah Social Services" while pursuing its attacks on the Lebanese government and its supporters.

Representing and quantifying the preferences of both sides (government and insurgents) and allowing them to change over time[28] is one of the main challenges in the implementation of such game/risk models. To do so requires a clear characterization of these preferences. One of the challenges of the counterterrorism model was to provide a sharp definition of the attributes of the government's utility function. The problem was not only to identify the attributes (e.g., the country's stability) but also to define a precise index that could be quantified through existing information. For the example presented here, these data were obtained through official sources in the Philippines. As mentioned earlier, the stability dimension, which was critical to the results, was measured by "the number of actionable human intelligence tips received by the government in the past n time units (here, three months) divided by number of insurgent attack initiatives." This meant, in effect, that the population is ready to work with the government while the insurgents are slowing down the pace of their attacks. There was thus an implicit submodel behind the definition of this attribute.

The nuclear nonproliferation study added to the counterterrorism model the possibility that options and preferences on both sides could evolve with internal and external changes of the environment. That model structure is essentially based on a large dynamic programming formulation, in which the possibility of all options and their evolutions are considered from the beginning of the time frame with a moving horizon. One of the main aspects of the dynamics of this case is the representation of the progress of nuclear weapon development within the country. To that effect, a new dynamic node was created and used in the influence diagram. That node had to include not only the technical progress of weapon development but also the political will to pursue that effort and thus the possibility of a change of leadership in the proliferating country, as was the case in the example of South Africa. In decision models, possible scenarios can be identified with the help of experts in diplomacy, intelligence, history, and political science. In the same way, the effects of the international environment were included as an external variable. The proliferation model was restricted to one country. In reality, it should be expanded to represent the interactions of several proliferating countries exchanging know-how and equipment.[29] The results (transitions among states) can then be included in the dynamic node. Further development of that model would require identification and characterization of common interests and alliances (with possible shifts) and of the signals to be observed and interpreted for the quantification of the corresponding transition probabilities.[30]

The fourth model, the management of project development, presents an interesting contrast to the adversarial situations of the national security models. It shows that the same concepts of merging a game analysis and a risk analysis model can apply to other types of situations, in which there is no open conflict but potentially divergent interests. In this case, the challenge was to anticipate, as in the other models, the effects of different management decisions on the behaviors of the principal's "adversary" (here a simple agent) and on the reliability of an engineered system. To do so, we combined a principal–agent model and a probabilistic risk analysis to show the risk reduction benefits of considering explicitly and systematically the probabilities and the consequences of various possible shortcuts.[31] Another critical element of this model formulation was to include the initial decision of the agent regarding the level of effort that he is willing to deploy because this choice clearly influences his chances of falling behind later, of shortcuts, and of increased failure risk.

The main simplifying assumption in this model was a one-time observation of the status of the project. In reality, large critical projects are reviewed regularly

[28] Here, by modifying the weights of the linear utility function.

[29] One example here is that of the AQ Khan network based in Pakistan and its dealings or its attempts to deal with other proliferating countries.

[30] A prime example at this time is that of North Korea and of the influence and role of several nations—China, Russia, South Korea, the United States, and others—that determine the intent and capabilities of that country to further develop its nuclear arsenal.

[31] In aircraft, for instance, the rigorous maintenance of critical systems is a priority given its greater importance to safety than the "small maintenance" of on-board amenities (even if in the end, their performance may affect the airline bottom line).

and so are more modest ones under responsible management; but the generalization of the framework to include a sequence of reviews is relatively straightforward, and this assumption allowed a simpler demonstration of the concepts through illustrative results.

In all the models presented here, influence diagrams played an important role in the problem structure and formulation, with the possibility of coupling them to represent dependencies of both parties' decisions and to extend them in the future to add external features that were not accounted for.

6.3. Time Factors and Games Dynamics

Time enters the problems addressed here in several ways, i.e., discounting for later effects of current decisions and timing of moves in the games. Discounting was explicitly included in the examples presented above. It was a key issue, for instance, in the counterterrorism model, where the goal was to assess the effects of long-term versus short-term investments on the country's stability. It was also critical to the management of an engineered system development, where the effects of shortcuts during that phase may not be observable until the systems' operations have started. The difficulty of course, is in the choice of the discount rate, whether it be the personal one of the agent involved (in project development) or the rates that effectively represent a country's preferences for different types of benefits of counterterrorism measures, now versus later. When the actors can be interviewed, they can be presented with intertemporal choices. Otherwise, one can only infer their discount rate from monetary interests (when applicable) or from observed behaviors.[32]

More complex perhaps are the dynamics of moves in games and risks, which entered the problems described here in two main ways: first, the evolution of a system and the timing of the outcomes (e.g., in the nuclear weapons' development process) and, second, the tempo of the games, which was assumed here for simplicity to be based on alternate moves at each time unit. The former—timing of outcomes—depends entirely on the system considered. For instance, in the illustrative case of defective constructions in a seismic area where a contractor has taken shortcuts, the failure risk is determined by the random time between earthquakes that will make the buildings fail with and without shortcuts. The latter, the game dynamics, was based here either on a single move or on alternate moves at each time unit. In reality, part of the strategy in a game might be to control the tempo.[33] One strategy may be to accelerate it to surprise the opponent or deny him the time to develop a response or on the contrary to slow down operations to give time to the other side to carefully weigh its options and their consequences in an attempt to avoid a conflict. This control of the tempo was not included in the models presented here. This would require defining a decision variable that represents, in effect, the choice of time units and a state variable that characterizes the time needed on both sides to develop a new strategy, make a move, escape, or attack.

A time-related dimension of preferences that is only implicitly accounted for in these models can be described as the patience or the resilience of the parties involved and the populations affected by a conflict. This issue is a complex one that in some cases involves deep cultural aspects. It enters the decision models through the variation of the preference functions over time given the circumstances, the outcomes of previous moves, and the morale of the different groups. This is relevant to the counterproliferation case when assessing, for instance, the effects of economic sanctions on nuclear weapons development and in the counterterrorism case when quantifying the effects of both the government's and insurgents' actions on the population well-being and stability.

One benefit of the three dynamic models presented here—counterterrorism, nuclear counterproliferation, and project management—is to emphasize the potential long-term effects of the decisions made along the way, especially when the short term may seem of utmost urgency.

[32] There may be a cultural aspect to the choice of a country discount rate, which could be influenced, for example, by an electoral schedule that favors short-term benefits, whereas others may have a longer view because of a longer leadership lifetime.

[33] For instance, the importance of tempo in aerial combat is illustrated by the work of John Boyd on Energy-Maneuverability and the Observation, Orientation, Decision, and Action loop (Coram 2002).

6.4. Information and Data

Two basic types of data are needed in game/risks models: probabilities and utilities from the perspective of the main actor regarding, first, his own decision and, second, those of his adversary. The preferences of U.S. decision makers (or the principals) can be encoded after the decision makers have been identified, according to the classic methods of decision analysis (for U.S. counterterrorism decisions, see, for example, Keeney 2007, Keeney and von Winterfeldt 2009). To capture the views of the adversaries, intelligence from all origins is a key source of data, in the case of weapons threats, nuclear counterproliferation, and counterterrorism. The information base includes, first, a deep background historical knowledge of the considered groups and countries and the history of prior probabilities. Current signals used to update the priors generally come from intelligence collection and open sources that often provide critical, easily accessible information. These include the local press, the media communications, and sometimes statements from the terrorists themselves, with the obvious possibility of disinformation. What the principal decision maker needs from these sources is an understanding of the capabilities, knowledge, and uncertainties of the adversaries as well as their intentions and preferences. For instance, as mentioned earlier, in the Philippine illustration of the counterterrorism model, information was gathered in the country from official sources. It included the history of the insurrection and the government's actions and the anticipated evolution of the conflict.

One difficulty in using intelligence information is to get a sense of uncertainties and an assessment of probabilities that often cannot be based on statistics and then to explain their validity to decision makers. The use of probability is not a traditional part of the intelligence culture where the analyst is often pressed to "make the call." As a consequence, it has sometimes been up to decision makers to imagine the possibility of alternative hypotheses, their chances, and their consequences. Things, however, are progressing, and the notion that prior probabilities can be updated based on new reports is making its way in that area (Willis 2007, von Winterfeldt and Paté-Cornell 2008).

In all cases considered here, the data are scarce and Bayesian probability is the only possible approach. The challenge in the implementation of these models is to set up an updating mechanism that allows updating of prior probabilities keeping in mind the background information that supports these priors to avoid accounting twice for specific facts and observations. One of the benefits of Bayesian models may thus be to temper a natural tendency to overemphasize the importance of the latest signal or news, forgetting the priors and what was known before.

6.5. Results and Insights

What each of these models provides is a perspective that may or may not have emerged explicitly from a purely qualitative perspective. The risk results are generally coupled with decision analysis models but are of different forms.

In the project management case, the result for each strategy is simply, in the end, the probability of system failure and the overall costs (a random variable) of managing an uncertain development process. Coupled with the preferences of the principal, it can provide support to management decisions. In the study of the relative threats of different terrorist weapons, the results were the probabilities that the groups considered were able to get and use each type of weapons. These probabilities were determined on the basis of a bounded rationality model, proportionally to the expected utility of the use of these weapons to the different groups, as assessed by the United States. In the end, their ranking was based on the damage that they could inflict and their disutility to the United States. In the counterterrorism case and for given investments of different time horizon, the result was the probability of failure of a strategy to stabilize the country, based on a measure of the stability attribute in the utility function of the government. The result of the nuclear counterproliferation model was the probability distribution, over a given time horizon, of the time to completion of a nuclear development program given a U.S. strategy to delay it. This result depended in part on the ability and the willingness of the country to develop that program, thus on internal factors such as its leadership, and on external influences such as the effects of U.S. strategies and the reactions of other countries.

In all cases, the risk results were thus based both on the probabilities and the preferences that influenced the decisions of both parties. To the degree that several of the games considered here have an international dimension, the cultural aspects of the preferences and the decisions made may have a major influence on the risk assessment.[34]

7. Conclusions

The use of game theory to assess the risks of different moves, especially when national security problems are involved, has a long history. The examples presented here are not meant to represent an exhaustive set of the possibilities in that field but to illustrate combinations of games and risks in different domains.

The main benefit of a risk assessment approach based on systems analysis is in its logics. It permits avoiding errors of intuition such as overlooking dependencies and ignoring or underestimating the weight of prior probabilities. Bayesian reasoning, which requires logical updating of information, can thus balance the natural instincts of decision makers to give excessive weight to the last piece of information received or to underestimate the long-term effects of their actions. In the cases considered here, the data relied in large part on expert opinions from various sources for each part of the problem. This formulation allows using the best information available in different domains when facing new situations and long-term consequences and trade-offs.

The main benefits of these models are thus in the insights that they can provide, some of which are not obvious or intuitive, such as the long-term costs of short-term strategic moves or the shadow cost of management constraints. As usual, these decision support models may be incomplete, for example, because the data are imperfect and new situations arise that may not be conceivable a priori. More often, the scenarios that have not been experienced before are considered too improbable to be of concern and are combinations of rare events. The use of probability allows anticipating these “perfect storms” and the moves of an intelligent adversary in a situation that has not yet been encountered. Clearly, the rare, true, “unknown unknown” (the unimaginable “black swan”) is not going to be captured, neither in models nor in strategic plans (Paté-Cornell 2012). The best approach in such cases includes improving the system’s robustness, monitoring precursors and signals, and quick—but thoughtful—responses (Larson 2004, Larson et al. 2005). Even then, the logical, systematic thinking provided by a decision/game analysis framework can be extremely useful in avoiding the problems of knee-jerk reactions.

The question in the end is whether educated intuition alone would provide a better answer. What is shown here is that in the strategic cases considered here and provided that the models’ formulation is appropriate, analytics combining games and risk analysis provides a powerful supplement to limited experience when both uncertainties and consequences can be overwhelming.

[34] An example relevant to terrorist choices may be the threat of suicide bombing from Islamist groups.

Acknowledgments

Part of this work was supported by the Burt and Deedee McMurtry Graduate Fellowship in the Department of Management Science and Engineering at Stanford University. Their support is gratefully acknowledged.

References

Bellman R (1957) *Dynamic Programming* (Princeton University Press, Princeton, NJ).

Bertsekas DP (2000) *Dynamic Programming and Optimal Control*, 2nd ed. (Athena Scientific, Nashua, NH).

Bier VM (2007) Choosing what to protect. *Risk Anal.* 27(3):607–620.

Bier VM, Azaiez MN, eds. (2008) *Game Theoretic Risk Analysis of Security Threats* (Springer, New York).

Bier VM, von Winterfeldt D, eds. (2007) Terrorism risk analysis. *Risk Anal.* 27(3):503–634.

Caswell DJ (2010) Analysis of national strategies for combating the proliferation of nuclear weapons. Unpublished doctoral thesis, Department of Management Science and Engineering, Stanford University, Stanford, CA.

Caswell DJ, Paté-Cornell ME (2011) Probabilistic analysis of a country’s program to acquire nuclear weapons. *Military Oper. Res.* 16(1):5–20.

Caswell DJ, Howard RA, Paté-Cornell ME (2011) Analysis of national strategies to counter a country’s nuclear weapons program. *Decision Anal.* 8(1):30–45.

Coram R (2002) *Boyd: The Fighter Pilot Who Changed the Art of War* (Little, Brown and Company, New York).

Cox LA (2009) Game theory and risk analysis. *Risk Anal.* 29(8):1062–1068.

de Finetti B (1970) *Theory of Probability* (Wiley, New York).

Dillon RL, Liebe RM, Bestafka T (2009) Risk-based decision making for terrorism applications. *Risk Anal.* 29(3):321–335.

Feng T, Keller LR (2006) A multiple-objective decision analysis for terrorism protection: Potassium iodide distribution in nuclear incidents. *Decision Anal.* 3(2):76–93.

Garber RG (2007) Corner cutting in complex engineering systems: A game theoretic and probabilistic modeling approach.

Unpublished doctoral thesis, Department of Management Science and Engineering, Stanford University, Stanford, CA.

Garber RG, Paté-Cornell ME (2006) Managing shortcuts in engineering systems and their safety effects: A management science perspective. Stamatelatos MG, Blackman HS, eds. *Proc. Eighth Internat. Conf. Probabilistic Safety and Management (PSAM)* (ASME Press, New York).

Garber RG, Paté-Cornell ME (2011) Shortcuts in complex engineering systems: A principal-agent approach to risk management. *Risk Anal.*, ePub ahead of print December 29, http://dx.doi.org/10.1111/j.1539-6924.2011.01736.x.

Gibbons R (1992) *Game Theory for Applied Economists* (Princeton University Press, Princeton, NJ).

Harasanyi JC (1959) A bargaining model for the cooperative N-person game. Tucker W, Luce RD, eds. *Contributions to the Theory of Games IV Annals of Mathematical Studies*, Vol. 40 (Princeton University Press, Princeton, NJ), 325–355.

Henley EJ, Kumamoto H (1992) *Probabilistic Risk Assessment* (IEEE Press, New York).

Howard R (1968) The foundations of decision analysis. *IEEE Trans. Systems, Sci., Cybernetics* 4(3):211–219.

Kahneman D (2003) Maps of bounded rationality: Psychology for behavioral economics. *Amer. Econom. Rev.* 93(5):1449–75.

Keeney RL (2007) Modeling values for counter-terrorism analysis. *Risk Anal.* 27(3):585–596.

Keeney RL, von Winterfeldt D (2009) A value model for evaluating homeland security decisions. *Risk Anal.* 29(3):438–456.

Kucik P (2007) Probabilistic modeling of insurgency. Unpublished doctoral thesis, Department of Management Science and Engineering, Stanford University, Stanford, CA.

Kucik P, Paté-Cornell ME (2012) Counter-insurgency: A risk-based analysis of different strategies. *Military Oper. Res.* Forthcoming.

Laffont J, Martimort D (2001) *The Theory of Incentives: The Principal-Agent Model* (Princeton University Press, Princeton, NJ).

Larson RC (2004) Decision models for emergency response planning. CREATE report, University of Southern California, Los Angeles.

Larson RC, Metzger MD, Cahn MF (2005) Emergency response for homeland security: Lessons learned and the need for analysis. CREATE report, University of Southern California, Los Angeles.

Lloyd J, Merrick JR (2011) Decision analysis applications in counterterrorism. *Wiley Encyclopedia of Operations Research and Management Science* (Wiley, New York).

Luce RD (1977) The choice axiom after twenty years. *J. Math. Psych.* 15(3):215–233.

Merrick JR, Parnell GS (2011) A comparative analysis of PRA and intelligent adversary methods for counterterrorism risk management. *Risk Anal.* 31(9):1488–1510.

Milgrom PR, Roberts J (1992) *Economics, Organization, and Management* (Prentice-Hall, Upper Saddle River, NJ).

Parnell GS, Smith CM, Moxley FI (2010) Intelligent adversary risk analysis: A bio-terrorism risk management model. *Risk Anal.* 30(1):32–48.

Paté-Cornell ME (2012) On "black swans" and "perfect storms": Risk analysis and management when statistics are not enough. *Risk Anal.*, ePub ahead of print March 2, http://dx.doi.org/10.1111/j.1539-6924.2011.01787.x.

Paté-Cornell ME, Guikema SD (2002) Probabilistic modeling of terrorist threats: A systems analysis approach to setting priorities among countermeasures. *Military Oper. Res.* 7(4):5–20.

Paté-Cornell ME, Garber R, Guikema S, Kucik P (2008) Games and risk analysis: Three examples of single and alternate moves. Bier V, Azaiez MN, eds. *Game Theoretic Risk Analysis of Security Threats* (Springer, New York), 147–175.

Raiffa H (1968) *Decision Analysis* (Addison-Wesley, Reading, MA).

Sagan S (1996–1997) Why do states build nuclear weapons? Three models in search of a bomb. *Internat. Security* 21(3):54–86.

Shoham Y, Leyton-Brown K (2009) *Multiagent Systems: Algorithmic, Game-Theoretic, and Logical Foundations* (Cambridge University Press, Cambridge, UK), 153–156.

Simon H (1957) *Models of Man, Social and Rational: Mathematical Essays on Rational Human Behavior in a Social Setting* (Wiley, New York).

von Neumann J, Morgenstern O (1947) *Theory of Games and Economic Behaviour*, 2nd ed. (Princeton University Press, Princeton, NJ).

von Winterfeldt D, Paté-Cornell ME (2008) Some progress in the analysis of intelligence information: Where we are and possible improvements. *Keynote Address to the Intelligence and Risk Anal. Sympos.* (Georgetown University, Washington, DC).

Willis HH (2007) Guiding resource allocations based on terrorism risk. *Risk Anal.* 27(3):597–606.