University of Massachusetts Amherst

Department of Resource Economics

Working Paper No. 2005-3

http://www.umass.edu/resec/workingpapers

INSPECTIONS TO AVERT TERRORISM: ROBUSTNESS UNDER SEVERE UNCERTAINTY

L. Joe Moffitt[1], John K. Stranlund[2] and Barry C. Field[3]

Abstract:

Protecting against terrorist attacks requires making decisions in a world in which attack probabilities are largely unknown. The potential for very large losses encourages a conservative perspective, in particular toward decisions that are robust. But robustness, in the sense of assurance against extreme outcomes, ordinarily is not the only desideratum in uncertain environments. We adopt Yakov Ben-Haim's (2001b) model of information gap decision making to investigate the problem of inspecting a number of similar targets when one of the targets may be attacked, but with unknown probability. We apply this to a problem of inspecting a sample of incoming shipping containers for a terrorist weapon. While it is always possible to lower the risk of a successful attack by inspecting more vessels, we show that robustness against the failure to guarantee a minimum level of expected utility might not be monotonic. Robustness modeling based on expected utility and incorporating inspection costs yields decision protocols that are a useful alternative to traditional risk analysis.

Keywords: Terrorism, Robustness, Severe Uncertainty, Port Security

[1] L. Joe Moffitt, Department of Resource Economics
University of Massachusetts, 212B Stockbridge Hall
Amherst, MA 01003-9246
E: moffitt@resecon.umass.edu P: 413-545-5719 F: 413-545-5853

[2] John K. Stranlund, Department of Resource Economics
University of Massachusetts, 214 Stockbridge Hall
Amherst, MA 01003-9246
E: stranlund@resecon.umass.edu P: 413-545-6328 F: 413-545-5853

[3] Barry C. Field, Department of Resource Economics
University of Massachusetts, 212F Stockbridge Hall
Amherst, MA 01003-9246
E: field@resecon.umass.edu P: 413-545-5709 F: 413-545-5853

March, 2005

INSPECTIONS TO AVERT TERRORISM: ROBUSTNESS UNDER SEVERE UNCERTAINTY

L. Joe Moffitt, John K. Stranlund, and Barry C. Field

Department of Resource Economics
University of Massachusetts, Amherst

Send correspondences to: Professor L. Joe Moffitt
Department of Resource Economics
212B Stockbridge Hall
University of Massachusetts
Amherst, MA 01002-9246
moffitt@resecon.umass.edu
413-545-5719

Acknowledgements: Funding for this research was provided by the U. S. Department of Agriculture under USDA/ERS/PREISM Cooperative Agreement No. 43-3AEM-4-80115. Additional support was provided by the Cooperative State Research Extension, Education Service, U. S. Department of Agriculture, Massachusetts Agricultural Experiment Station under Project No. MAS00861

INSPECTIONS TO AVERT TERRORISM: ROBUSTNESS UNDER SEVERE UNCERTAINTY

Abstract: Protecting against terrorist attacks requires making decisions in a world in which attack probabilities are largely unknown. The potential for very large losses encourages a conservative perspective, in particular toward decisions that are robust. But robustness, in the sense of assurance against extreme outcomes, ordinarily is not the only desideratum in uncertain environments. We adopt Yakov Ben-Haim's (2001b) model of information gap decision making to investigate the problem of inspecting a number of similar targets when one of the targets may be attacked, but with unknown probability. We apply this to a problem of inspecting a sample of incoming shipping containers for a terrorist weapon. While it is always possible to lower the risk of a successful attack by inspecting more vessels, we show that robustness against the failure to guarantee a minimum level of expected utility might not be monotonic. Robustness modeling based on expected utility and incorporating inspection costs yields decision protocols that are a useful alternative to traditional risk analysis.

Keywords: Terrorism, Robustness, Severe Uncertainty, Port Security

1. Introduction

Terrorism involves unorthodox attacks, primarily on civilians, with the aim of producing damage, and especially fear, within the targeted population. There are several ways of reducing its potential impacts: neutralizing the terrorists before they act; intercepting terrorist actions after they commence but before they are actually consummated; and hardening potential targets. This paper is about the second of these options, in particular that of intercepting a surreptitious terrorist attack that may be launched against one of some number of similar targets. Examples abound. One is the much-commented upon problem of incoming shipping containers. Millions arrive each year into the various ports of the country. A substantial undetected weapon in one of them could cause great damage. Another example is reservoirs; there are many thousands scattered around the country, any one of which could be attacked with a biological or chemical agent. Still another example is aircraft; with thousands of passenger and cargo flights every day, history has shown us that an attack on just one can produce enormous damage if it succeeds. Agricultural bioterrorism is still another example. For any type of output – wheat, corn, a certain type of livestock, etc., there are hundreds or perhaps thousands of individual farms against which an attack could be launched with the intent of introducing a pathogen that would spread to other farms or a contaminant that would create fear among consumers.

Modeling this as a case of risk management implies knowing, or assuming, something about attack probabilities and the effectiveness of steps that might be taken to reduce the ultimate probabilities of damage. There has been work to develop and examine time series of terrorist events over reasonably long periods (Enders and Sandler (2002); Mickolus et al. (1989, 1993); Enders et al. (1992); O'Brien (1996)). But it is not straightforward to turn frequencies into attack probabilities for specific targets. Use of expert judgment for the purposes of risk assessment can also be problematic both from methodological and experiential perspectives. There is no formally established methodology for treating expert judgment, and Bayesian and other approaches suffer from limitations in practical application (Ouchi (2004)). Risk assessment in practice has proved to be difficult, time consuming, and expensive in some important applications and virtually impossible in others. What this strongly suggests is that it may not be useful to analyze the defense against terrorism as if they were decisions involving gambles with known probabilities. In this paper, therefore, we present an analysis of decisions to intercept terrorist actions that can be taken without knowing, or assuming, anything about the probability distributions associated with terrorist actions, that is, under conditions of true uncertainty.

Of course some tools have been developed for addressing situations of true uncertainty; this includes the maximin, maximax, Laplace, and Hurwitc criteria (see e.g., Render et al. (2003)). While none of these criteria require knowledge of probability distributions for application, the first two represent polar extremes in terms of optimism and pessimism while the latter two require information similar to probabilities in order to be applied. Similarly, quantification of other notions related to uncertainty such as ignorance and surprise have also required specification of functions confined to the unit interval (Katzner (1998); Horan et al. (2002)). Additionally, Kelsey (1993) developed a distinctive decision theory requiring a ranking of event probabilities rather than a specific probability distribution. Perhaps for these reasons, none of these decision criteria under uncertainty have achieved the widespread application in economics afforded traditional risk criteria.

In the case of terrorism, the possibility that losses could be large encourages a conservative outlook, as is inherent in the maximin criterion. Maximin is maximally robust in the sense that it guarantees a result that equals or exceeds the worst of the possible outcomes that might result from a chosen strategy. But robustness is not everything; in return for better performance on some other important parameter one may be willing to give up some degree of

robustness. This implies a decision model which, though featuring robustness, accommodates tradeoffs with other parameters when the situation warrants.

Recently Ben-Haim (1999) has developed a theory of decision-making under true uncertainty that he calls information (info)-gap decision theory (Ben-Haim (1994); Ben-Haim (1999); Ben-Haim (2001a)). Info-gap decision theory is designed for decisions in which probability distributions for uncontrolled events are not available. The essence of info-gap is pursuit of a performance requirement over the largest possible "range" of uncontrolled events. There have been a number of applications of the info-gap theory to problems ranging from selection of financial portfolios to optimal search in predator-prey systems (Ben-Haim (2001b)).

In the next section we generalize info-gap theory with expected utility as a measure of performance. In section 3 we use this approach to model a problem of protecting against terrorism: inspecting a large number of container ships for the presence of materials which, if not detected, would produce great damage in a target population. Uncertainty in this problem is about the probability that harmful material has been placed on one of the ships. We do not specify a utility function for the decision maker; rather we simply assume that the decision maker is risk averse, perhaps weakly. Our primary motivation with this model is to characterize the trade-off between costly inspections and robustness. Robustness in our problem is the maximum range of the unknown probability of a terrorist attack for which a performance criterion is satisfied. Thus, it is a notion of security against failing to meet a performance criterion. Security in our formulation has two dimensions: security against failing to avert a successful terrorist attack with some low probability, and security against failing to meet a minimum level of expected utility. As one would intuit, we show that security against failing to avert a terrorist attack is increasing in the number of inspected vessels. However, when the problem of robustness is posed in the economic terms of guaranteeing a minimum level of expected utility for a decision maker with an unknown degree of risk aversion, there could be a potentially large range of numbers of inspections for which more inspections leave the decision maker less secure. In some situations, therefore, a decision maker may face a difficult trade-off: increasing inspections to increase the level of security against a successful terrorist attack may reduce security against failing to meet a minimum level of expected utility.

In section 4 we conduct a series of simulations to investigate the effects of problem parameters on robustness against failing to meet a minimum level of expected utility. We find

that for a given number of inspections, robustness is decreasing in the size of the loss from a successful terrorist attack, a critical failure probability, and the elasticity of the inspection costs. We also investigate the effects of these parameters on the monotonicity of robustness. We conclude in section 5.

2. Uncertainty and Robustness

Ben-Haim's (1999) info-gap decision theory is built on the specification of four components: the system model, the performance requirement, the uncertainty model, and the robustness function. In his decision framework, the system model expresses the structure of rewards that follows from decisions and events. For example, it might be the structure of net benefits accruing to a decision maker on the basis of their choices of alternative levels of inputs, together with uncertain events in the environment. The performance requirement is some particular reward level deemed necessary in a given decision problem. Some minimum level of net benefits might be chosen as a performance requirement, for example. The uncertainty model consists of a family of convex, nested sets where the elements of each set are possible realizations of uncertain events affecting rewards. In this uncertainty framework, the higher the degree of nesting, the greater the uncertainty about events. The robustness function shows the relationship between decision variables and the greatest level of uncertainty at which the performance requirement will be achieved; it is the subject of maximization to identify the optimal robust decision. In addition, Ben-Haim distinguishes between the info-gap models where probability is not regarded as an appropriate uncertainty concept (e.g., cases involving novel events) versus "hybrid" cases where probability is an applicable concept but is unknown and difficult to assess.

While preserving the info-gap philosophy of uncertainty and robustness, we generalize the theory's components to include both the basic info-gap and hybrid cases and to permit a less restrictive characterization of uncertainty. Let $v \in V$ denote possible realizations of uncertain elements in a decision problems where V is any set, and let $x \in X$ be a vector of decision variables in the problem with $x \in R^n$. The set V can encompass uncertain elements including parameters, exogenous variables, probability distributions, etc. The system model reflects the structure of rewards depending on both x and v, while the performance requirement is a predetermined reward level. Uncertainty about possible realizations of elements affecting rewards is $\mathcal{U} = \mathcal{P}(V)$, where $\mathcal{P}(\cdot)$ denotes the power set (all possible subsets) of V. Note that the

elements of $\mathcal{U}$ consist of possible realizations of uncertain problem elements; however, they need not be convex. Given an ordering relation on $\mathcal{U}$, the robustness function, $\alpha(x)$, is a set-valued function $\alpha : X \to \mathcal{P}(V)$ describing the largest element of $\mathcal{U}$ that satisfies the performance requirement conditional on decision x. An ordering relation is needed to compare elements of $\mathcal{U}$ that satisfy the performance requirement, and reflects the meaning of robustness in the decision problem. The robustness function indicates the most robust element of $\mathcal{U}$, conditional on x that satisfies the performance requirement. The optimal robust decision is $\arg\max_{x \in X} \alpha(x)$; that is, the value of the decision variable that leads to a maximum of the robustness function.

The following decision problem will help to make the components of our decision framework more complete. Let the reward be a random variable v, and $U(v)$ be the decision maker's von Neuman-Morgenstern utility function. The reward is determined by the level of a decision variable, x, and an unknown conditional probability density function, $f(v \mid x)$, that represents the uncertainty inherent in the decision maker's environment. Let $g(v)$ be a probability density function for v used in specifying a performance requirement. The *system model* defines rewards and is taken to be expected utility, $\bar{U}_{(\cdot)}$, where the expectation is evaluated with respect to the subscripted probability density function. The *uncertainty model*, $\mathcal{U}$, consists of the power set of conditional probability density functions, $\{f(v \mid x)\}$. The *robustness function*, $\alpha(x)$, indicates the largest subset of $\mathcal{U}$ (the ordering relation is assumed to be the number of elements) over which the *performance requirement* (smallest acceptable expected reward) $\bar{U}_g$ will be achieved.

The *robust optimal decision* can be found by solving

(1) $\underset{x \in X}{\textit{Maximize}} \quad \alpha(x)$

(2) $\textit{Subject to} \quad \bar{U}_f \geq \bar{U}_g$

(3) $\int f(v \mid x) dv = 1$

(4) $f(v \mid x) \geq 0$

(5) $x \in X$,

where the set X reflects any constraints on x other than the performance requirement and those

constraints on the conditional density, $f(v \mid x)$, related to the definition of a probability density function. Assuming a solution exists, the solution to (1) - (5) provides a specific value of the decision variable, x^*, associated conditional density function, $f(v \mid x^*)$, and maximum robustness, $\alpha^* = \alpha(x^*)$. Given an appropriate specification of robustness, the performance requirement will be achieved not only under $f(v \mid x^*)$, but also under perhaps a wide range of related densities.

As it stands, the model (1) - (5) poses a difficult constrained optimization problem. The two key elements that are needed to implement (1) - (5) are specifications of the robustness objective function and the performance requirement, which is shown in (2) as a constraint on expected utility. As demonstrated in the next section, it is possible to make meaningful specifications for both of these elements in the context of robust inspections of ships for a terrorist weapon.

3. Robustness and Inspections at Containerports

In this section we illustrate the use of the model developed in the previous section for allocating scarce resources to manage a security risk under uncertainty. Risks are managed through detection effort consisting of inspections for a terrorist weapon of trade shipments to an international containerport. Port security is a complex problem involving a variety of functions; random inspections of container cargo may be one part of an efficient policy (see e.g., Harrald et al. (2003)). Hence, use here of the model developed in the previous section is intended to focus on a robust detection effort. In particular we are interested in characterizing the trade-off between costly inspections and robustness; that is, how the largest range of uncertainty under which a performance criterion is satisfied varies with the number of inspected vessels.

Suppose that *B* denote the benefit due to shipping activity at a containerport without a security threat; *p* denotes the probability that a weapon is present on one of *N* vessels that will call at the port, and *L* denotes the cost of failure to prevent passage of this weapon through the port. The port manager's decision is to choose the number of random inspections of incoming vessels to prevent passage of the weapon through the port. A traditional approach would evaluate the opportunity costs of inspection compared to the expected benefits of this action, where these expected benefits would depend critically on the probability of a terrorist attack. We will

proceed, however, with an assumption that we do not know what this probability is, but the port manager must choose the number of vessels to inspect in spite of this uncertainty. Let n denote the number of vessels inspected for these materials at cost $C(n)$, with $C'(n) > 0$ and $C'' \geq 0$. The probability that there is a weapon on one of the vessels, p, is completely unknown; hence, we adopt model (1)—(5) to investigate the trade-off between inspections and robustness.

Given inspections, n, and a probability that a weapon is aboard one of the vessels, p, the conditional probability density function, $f(v \mid n, p)$, for net benefit, v, is

$$(6) \qquad f(v \mid n, p) = \begin{cases} 1 - \dfrac{p(N-n)}{N} & \text{if } v = B - C(n) \\ \dfrac{p(N-n)}{N} & \text{if } v = B - L - C(n). \end{cases}$$

The uncertainty model is the set $\{f(v \mid n, p),\ n \in [0, N],\ p \in [0,1]\}$, and all its subsets. Given N, the uncertainty model consists of a set of probability density functions characterized by the inspection decision, n, and the unknown parameter, p, confined to the unit interval. Since uncertainty in this context is about the real value of p, the robustness function can be specified meaningfully as that value. Note that $p(N-n)/N$ is the probability that a weapon passes through the port undetected. We will call this the failure probability and denote it by π. Given n and p, the decision makers' expected utility is

$$(7) \qquad \bar{U}_f = U\big(B - C(n)\big)\big(1 - p(N-n)/N\big) + U\big(B - L - C(n)\big)\big(p(N-n)/N\big).$$

The performance criterion for this problem is that $\bar{U}_f \geq \bar{U}_g$. Two modeling decisions must be made at this point to specify the performance criterion. First, we need to specify the smallest acceptable expected utility, $\bar{U}_g$. In addition we need to specify the decision maker's utility function. This is a bit troubling, because in most cases the decision maker's utility function will be unknown, either to him or her or to the analyst. Our approach is to assume that the decision maker's utility function is unknown, but that it is known that he or she is risk averse

(perhaps weakly). Then we can appeal to well known results from the theory of stochastic dominance to specify the performance criterion.

First let us model the smallest acceptable expected utility, $\bar{U}_g$. In principle $\bar{U}_g$ can be any level deemed appropriate by the decision maker. We, however, derive $\bar{U}_g$ from another robustness/inspections tradeoff, but one that lacks economic content. Gauging the performance of stochastic systems by the probability of failure and establishing a performance requirement in terms of failure probability are common. Imagine a robust decision to hold the failure probability to be no more than some critical value, π_c, given that the probability that damaging material is on board one of the vessels is no more than p_c. In effect, the decision maker is saying, given that I believe that the probability that a weapon is on one of the vessels is no more than p_c, I will choose the number of inspections to make sure that my failure probability does not exceed π_c. We assume throughout that $p_c > \pi_c$. Then, the performance requirement for robust inspections in terms of the unknown probability of a weapon passing through the port undetected is $\pi = p(N-n)/N \le \pi_c,$ for $p \in [0, p_c]$.

As noted above the robustness function can be specified simply with respect to p. For this problem the robustness function is

$$(8) \qquad p(n, \pi_c, p_c) = \max\left\{ p \mid \max_{p \in [0, p_c]} p(N-n)/N \le \pi_c,\ n \in [0, N] \right\}.$$

Maximal robustness given inspections and the performance criterion requires choosing p so that the performance criterion is exactly satisfied. Therefore, the solution to (8) is

$$(9) \qquad p(n, \pi_c, p_c) = N\pi_c/(N-n),\ p \in [0, p_c],\ n \in [0, N].$$

The robustness function indicates security against failing to hold the probability of a successful terrorist attack to no more than the critical failure probability. Given inspections, n, if the actual probability of a terrorist attack is less than $p(n, \pi_c, p_c)$, then the probability of a successful attack is less than the critical failure probability, π_c; but if the actual probability of an

attack is greater than $p(n, \pi_c, p_c)$ the probability of a successful attack will exceed π_c. Thus, higher values of robustness indicate greater security against failing to hold the probability of terrorist's success to no more than the critical failure probability.

Note that $p(n, \pi_c, p_c)$ is monotonically increasing in inspections. That is, security against failing to hold the probability of a successful attack to no more than the critical failure probability is increasing in the number of inspected vessels. This is a rather intuitive conclusion—more inspections increase the range of attack probabilities for which the required failure probability is not exceeded. Choosing inspections to maximize robustness in this context is to simply choose $n_c = N(p_c - \pi_c)/p_c$ so that $p(n, \pi_c, p_c) = p_c$. That is, the strategy of inspecting n_c vessels guarantees that the critical failure probability is not exceeded for any chance that an attack has occurred up to the constraint on this chance.[1]

Now define the probability density function for payoffs, *v*, with inspections, $n_c = N(p_c - \pi_c)/p_c$, evaluated at maximum constrained robustness, p_c:

$$(10) \qquad g(v \mid n_c, p_c) = \begin{cases} 1 - \pi_c & \text{if } v = B - C(n_c) \\ \pi_c & \text{if } v = B - L - C(n_c). \end{cases}$$

Expected utility of $g(v \mid n_c, p_c)$ is

$$(11) \qquad \bar{U}_g = U\left(B - C(n_c)\right)\left(1 - \pi_c\right) + U\left(B - L - C(n_c)\right)\pi_c.$$[2]

Now let us turn to guaranteeing that $\bar{U}_f \geq \bar{U}_g$ when *U* is unknown. Assuming that the

---

[1] Note that n_c is decreasing in π_c and increasing in p_c. Thus, inspections to meet the performance criterion are decreasing in the maximum allowable failure probability, and increasing in the upper bound the decision maker places on the probability that harmful material is on one of the ships.

[2] It is easy to demonstrate that $\bar{U}_g$ is monotonically decreasing in p_c. This is intuitive. If the decision maker considers a larger range of probabilities that harmful material is on board one of the vessels, then more inspections are needed to make sure that the failure probability does not exceed π_c. Thus, a higher p_c implies higher inspection costs and lower expected utility of $g(v \mid n_c, p_c)$. It is not possible to determine how $\bar{U}_g$ changes with the critical failure probability π_c without additional structure on the decision makers' utility function.

decision maker is risk averse, then $\bar{U}_f \geq \bar{U}_g$ can be replaced with a condition based on second-degree stochastic dominance (SSD). Let the cumulative distribution functions of $f(v \mid n, p)$ and $g(v \mid n_c, p_c)$ be $F(v \mid n, p)$ and $G(v \mid n_c, p_c)$, respectively. Then, $f(v \mid n, p)$ dominates $g(v \mid n_c, p_c)$ in the sense of SSD if and only if

$$(12) \qquad \int_{-\infty}^{v} \big(G(t \mid n_c, p_c) - F(t \mid n, p)\big) dt \geq 0, \text{ for all } v.$$

Furthermore, if $f(v \mid n, p)$ dominates $g(v \mid n_c, p_c)$, then $f(v \mid n, p)$ is at least as preferred to $g(v \mid n_c, p_c)$ by any risk averse decision maker (Hadar and Russell 1969, 1971). Thus, when a risk-averse decision maker's utility function is unknown, the performance requirement, $\bar{U}_f \geq \bar{U}_g$, can be replaced with (12).

The cumulative distribution functions in this problem are step functions corresponding to the discrete probability density functions specified in (6) and (10). An example is provided in Figure 1. Note that (12) holds if and only if $n \leq n_c$ and $B \leq A$. The latter inequality is

$$\left(\frac{p(N-n)}{N} - \pi_c\right)\big((B - C(n_c)) - (B - L - C(n))\big) \leq \pi_c \big((B - L - C(n)) - (B - L - C(n_c))\big),$$

which simplifies to $\big(p(N-n)/N\big)\big(L + C(n) - C(n_c)\big) - \pi_c L \leq 0.$

We are now ready to specify the robustness function for the port manager. It is

$$(13) \qquad p(n, L, C, \pi_c, p_c) =$$

$$\max\left\{p \mid \max_{p \in [0, p_c]} \big(p(N-n)/N\big)\big(L + C(n) - C(n_c)\big) - \pi_c L \leq 0,\ n \in [0, N(p_c - \pi_c)/p_c]\right\}.$$

In this problem the robustness function depends not only on the number of inspections, *n*, but also the potential loss from a weapon passing through the port undetected, *L*, the inspection cost function, *C*, the critical failure probability used to specify the performance criterion, and the upper bound the decision maker places on the probability that a weapon is present on one of the

vessels, p_c. Given these conditions of the problem, the robustness function specifies maximal values of p for each value of n for which any risk averse decision maker prefers the probability density function $f(v \mid n, p)$ to $g(v \mid n_c, p_c)$. Thus maximizing robustness given n is constrained by the SSD conditions $n \in [0, n_c = N(p_c - \pi_c)/p_c]$ and $\big(p(N-n)/N\big)\big(L + C(n) - C(n_c)\big) - \pi_c L \leq 0$. Since maximizing p, given n, requires that this latter constraint hold with equality when $p \in [0, p_c]$, the robustness function is

$$(14) \qquad p(n, L, C, \pi_c, p_c) = \frac{N\pi_c L}{\big(N-n\big)\big(L + C(n) - C\big(N(p_c - \pi_c)/p_c\big)\big)} \in [0, p_c],\ n \in [0, N(p_c - \pi_c)/p_c].^3$$

Specifying the decision maker's performance criterion in terms of a minimum level of expected utility changes the notion of security against failure. Given inspections, n, the robustness function indicates the largest range of the unknown probability of a terrorist attack for which the expected utility of any risk averse decision maker does not fall below the expected utility of guaranteeing that the probability of a successful attack does not exceed some critical failure probability. Thus, greater levels of $p(n, L, C, \pi_c, p_c)$ indicate that the decision maker is more secure against failing to guarantee the minimum level of expected utility.

Not surprisingly, a solution to choosing n to maximize $p(n, L, C, \pi_c)$ is to inspect $n_c = N(p_c - \pi_c)/p_c$ vessels to induce robustness $p = p_c$. Of course, this is the robust optimal strategy for making sure that the critical failure probability, π_c, is not exceeded. Consequently this is not a very informative strategy for a decision maker because it has no economic content. Moreover, this strategy may be unreasonably costly. A decision maker will want a full accounting of the fundamental trade-off between robustness against a terrorist attack and the costly activity of inspecting cargo vessels. In the next section we pursue this issue by examining the characteristics of $p(n, L, C, \pi_c, p_c)$.

[3] Note that any fixed costs of inspections will cancel out in $p(n, L, C, \pi_c)$. Thus, robustness in this context does not depend on fixed inspection costs, only variable costs.

4. Robustness Against a Terrorist Attack

In this section we examine the characteristics of the robustness function, particularly how it varies with inspections and alternative parameter values. It is useful at this point to put this into context. Our ultimate search is for a way to offer guidance to a port manager who must make decisions with very little information to go on. In particular we assume he, or she, does not know the attack probabilities they face, and in fact knows little about their own utility function, other than that they are risk averse.

Given inspections, n, $p(n, L, C, \pi_c, p_c)$ is the maximum probability of an attack for which the port manager is guaranteed a minimum expected utility. Figure 2 shows the robustness function under the following assumptions: $B = 25\times10^9$; $L = 1\times10^9$; $C(n) = 1000n^2$; $N = 1000$; $\pi_c = 0.05$, and $p_c = 1.0$. We do not include fixed inspection costs, because we've already noted that robustness does not depend on these costs. Moreover, our assumption that $p_c = 1.0$ means that the decision maker does not place an upper bound the range of attack probabilities that he or she is considering. The most obvious feature of the relationship between robustness and inspections in Figure 2 is that it is not monotonic; it has a local maximum at $\overline{n}$, and a global maximum at $n_c = N(p_c - \pi_c)/p_c = N(1-\pi_c)$.

At first blush, one might expect that robustness would increase as the number of inspected vessels increases, but this is clearly not always the case. We have been using robustness to indicate the decision maker's security against failure. Recall that security in our formulation has two dimensions: security against failing to guarantee that the probability of a successful attack does not exceed some low probability, and security against failing to meet a minimum level of expected utility. The former is clearly increasing in the number of inspected vessels because, for some attack probability, more inspections imply a lower probability of a successful attack. On the other hand, Figure 2 makes it clear that security against failing to guarantee a minimum level of expected utility may not be monotonic in inspections. Thus, when the problem of robustness is posed in the economic terms of benefits and costs under unspecified risk aversion, there could be a potentially large range of numbers of inspections for which more inspections leave the decision maker less secure. In some situations, therefore, a decision maker may face a difficult trade-off: increasing inspections to increase the level of security against a

successful terrorist attack may reduce security against failing to meet a minimum level of expected utility.

Let us investigate the non-monotonicity of $p(n, L, C, \pi_c, p_c)$ more thoroughly. Ignoring the boundary constraints on the robustness function for the moment, from (14) obtain

$$\frac{\partial p(n, L, C, \pi_c, p_c)}{\partial n} = \frac{\pi_c NL\left\{L - C\left(N(p_c - \pi_c)/p_c\right) + C(n) - C'(n)(N-n)\right\}}{\left[(N-n)\left(L - C\left(N(p_c - \pi_c)/p_c\right) + C(n)\right)\right]^2}.$$

Clearly, robustness is increasing in *n* if and only if

(15) $$L - C\left(N(p_c - \pi_c)/p_c\right) > C'(n)(N-n) - C(n).$$

On the left hand side of (15), $L - C\left(N(p_c - \pi_c)/p_c\right)$ is a constant: the cost term is the total cost of inspecting enough vessels to guarantee that the failure probability does not exceed π_c, for any $p \in [0, p_c]$. For our numerical example, $L - C\left(N(p_c - \pi_c)/p_c\right) = \$97.5$ million. On the right hand side of (15) we have $C'(n)(N-n) - C(n)$. For our example: $C'(n)(N-n) - C(n)$ is equal to zero when *n* is zero; it is strictly concave, reaching a maximum of $333.33 million at about 333 inspected vessels, and is negative for about 667 inspected vessels and greater. Clearly, the robustness function is not monotonic if and only if the maximum of $C'(n)(N-n) - C(n)$ exceeds $L - C\left(N(p_c - \pi_c)/p_c\right)$ as it does in our example. Note further that for low *n* $L - C\left(N(p_c - \pi_c)/p_c\right) > C'(n)(N-n) - C(n)$, so robustness is increasing. At some level ($\overline{n}$ in Figure 2), $C'(n)(N-n) - C(n)$ rises above $L - C\left(N(p_c - \pi_c)/p_c\right)$, driving robustness down. The final increase in robustness comes about because $C'(n)(N-n) - C(n)$ falls below $L - C\left(N(p_c - \pi_c)/p_c\right)$ and rather quickly becomes negative, driving robustness ultimately up to $p_c = 1$.

It is clear that the term $L - C\left(N(p_c - \pi_c)/p_c\right)$ has an important impact on the robustness function. Therefore, the robustness function is determined, in part, by the levels of the potential loss from an attack, *L*; the range of attack probabilities that the decision maker is willing to

allow, [0, p_c], and the critical failure probability used to determine the decision maker's performance criterion, π_c. Let us examine the effects of the first two parameters on the robustness function.

It is easy to demonstrate that the robustness function of (14) is montonically decreasing in the potential damage. Figure 3 depicts three robustness functions for three different levels of loss L: L(*med*) = \$1 billion; L(*large*) = \$1.3 billion; and L(*small*) = \$0.98 billion. Clearly, for any number of inspections, robustness is lower the larger is the damage from a successful attack. Thus, the range of probabilities over which the port manager meets or exceeds his or her chosen level of minimum expected utility is smaller the larger the damage from a successful attack.

Note also that the monotonicity of the robustness function is associated with the size of potential damage—relatively large levels of potential loss imply that the robustness function is monotonically increasing. This effect can be deduced directly from (15). Recall that the robustness function is monotonically increasing if and only if $L - C\left(N(p_c - \pi_c)/p_c\right)$ is greater than the maximum of $C'(n)(N-n) - C(n)$. With L(*large*) = \$1.3 billion, $L - C\left(N(p_c - \pi_c)/p_c\right)$ = \$397.5 million while $\max\left[C'(n)(N-n) - C(n)\right]$ = \$333.33 million.

Achievable levels of robustness are also related to the minimum level of performance that is required. In general, the higher this minimum performance the lower the attainable level of robustness. We have set the performance requirement in terms of a level of expected utility, in particular that level of utility achieved with a robustness of unity under a critical failure rate of 0.05. One could argue that setting p = 1.0 is unnecessarily conservative, that the authorities may be confident in thinking that the true attack probability is, say, no greater than 0.5, or perhaps even lower. Thus, although they do not know the probability, they can, with some confidence, give it a realistic upper bound.

This argues for changing the minimum expected utility, specifying it as the expected utility of guaranteeing the failure rate of no more than 0.05, but a maximum value of the real attack probability, p_c, held to be realistic by the authorities. Reducing p_c reduces the number of vessels that must be inspected to hold the probability of a successful attack to no more than a given value. That is $N(p_c - \pi_c)/p_c$ declines as p_c is reduced, which raises the minimum level of

expected utility the decision maker specifies in his or her performance criterion.[4] Consequently, for any level of inspections, robustness is lower for a lower maximum value of possible attack probabilities that the decision maker deems reasonable. Figure 4 confirms that the robustness function is monotonically decreasing in p_c.

Note also that the monotonicity of $p(n, L, C, \pi_c, p_c)$ is related to the maximum value of the attack probability—very low maximum levels of this probability tend to make robustness monotonic in inspections. With $p_c = 0.2$, only 750 vessels need to be inspected to guarantee that the failure probability does not exceed 0.05 for possible attack probabilities between 0 and 0.2. The cost of inspecting this many vessels is $C\left(N(p_c - \pi_c)/p_c\right) = \$562.5$ million and $L - C\left(N(p_c - \pi_c)/p_c\right) = \$437.5$ million. Since this is larger than $\max\left[C'(n)(N-n) - C(n)\right] =$ \$333.33 million, the robustness function is monotonically increasing in inspections.

5. Conclusions

In this paper we have sought to find a new way of modeling decisions in situations where the probabilities of certain key precipitating events are unknown. We have modified the info-gap model of Ben-Haim (2001b) to model inspection decisions for incoming terrorist weapons when the probability that a weapon is actually on an incoming vessel is unknown. The model proceeds by using the concept of robustness, defined as a level of assurance that an outcome will be no worse for the decision maker than some chosen critical value of performance. In our case the critical value is defined in terms of expected utility of guaranteeing that the probability of failing to avert a successful terrorist attack does not exceed some low probability. The decision maker chooses the number of incoming vessels to inspect in the light of the implications of this for the level of robustness that is attainable relative to this critical value. We show that this approach does offer a way of characterizing trade-offs despite the ignorance of attack probabilities. Perhaps our most interesting finding is that, while security against failing to hold the probability of a successful terrorist attack to no more than some critical failure probability is increasing in the number of inspected vessels, security against the failure of a decision maker with an unknown degree of risk aversion to guarantee a minimum level of expected utility may not be monotonic. We also show that the achievable levels of robustness are affected by many factors,

[4] It is evident that the minimum level of expected utility could be increased in two ways: by lowering the critical failure rate, or by maintaining the critical failure rate but reducing p_c. We have chosen the latter.

including inspection costs, the size of the prospective losses if an attack succeeds, and the level of expected utility taken as the critical performance level.

REFERENCES

Ben-Haim, Y. "Convex-Models of Uncertainty: Applications and Implications." *Erkenntnis*. 41(1994): 139-156.

Ben-Haim, Y. "Set-Models of Information Gap Uncertainty: Axioms and an Inference Scheme." *Journal of the Franklin Institute*. 336(1999): 1093-1117.

Ben-Haim, Y. "Decision Trade-Offs Under Severe Info-Gap Uncertainty." *2nd International Symposium on Imprecise Probabilities and Their Applications*. (2001a). 8 pp.

Ben-Haim, Y. *Information-Gap Decision Theory*. Academic Press. 2001b. 346 pp.

Enders, W., and T. Sandler. "Patterns of Transnational Terrorism, 1970-99: Alternative Times Series Estimates." *International Studies Quarterly* 46 (2002), 145-165.

Enders, W., G. F. Parise and T. Sandler. "A Time Series Analysis of Transnational Terrorism: Trends and Analysis." *Defence Economics* 3 (1992), 305-320.

Hadar, J. and W. R. Russell. "Rules for Ordering Uncertain Prospects." *American Economic Review* 59 (1969), 25-34.

Hadar, J. and W. R. Russell. "Stochastic Dominance and Diversification." *Journal of Economic Theory* 3 (1971), 288-305.

Harrald, J. R., H. W. Stephens, and J. R. van Dorp. "A Framework for Sustainable Port Security." *Journal of Homeland Security and Emergency Management*: Vol. 1; No. 2, Article 12 (2004). http://www.bepress.com/jhsem/vol1/iss2/12

Horan, R. D., C. Perrings, F. Lupi, and E. H. Bulte. "Biological Pollution Prevention Strategies Under Ignorance: The Case of Invasive Species." *American Journal of Agricultural Economics*. 84(2002): 1303-1310.

Katzner, D. W. *Time, Ignorance, and Uncertainty in Economic Models*. The University of Michigan Press. 1998.

Kelsey, D. "Choice Under Partial Uncertainty." *International Economic Review*. 34(1993): 297-308.

Mickolus, E. F., T. Sandler, J. M. Murdock, and P. Fleming. *International Terrorism: Attributes of Terrorist Events, 1978-1987.* (*ITERATE 3*). Dunn Loring, VA. Vinyard Software. 1989.

Mickolus, E. F., T. Sandler, J. M. Murdock, and P. Fleming. *International Terrorism: Attributes of Terrorist Events, 1988-1991.* (*ITERATE 4*). Dunn Loring, VA. Vinyard Software. 1993.

O'Brien, S. P. "Foreign Policy Crisis and the Resort to Terrorism: A Time Series Analysis of Conflict Linkages." *Journal of Conflict Resolution* 41 (1996), 320-335.

Ouchi, F. "A Literature Review on the Use of Expert Opinion in Probabilistic Risk Analysis." World Bank Policy Research Working Paper 3201. February 2004.

Render, B., R. M. Stair, Jr., and M. E. Hanna. *Quantitative Analysis for Management*. Eighth edition. Englewood Cliffs, NJ: Prentice Hall, 2003.

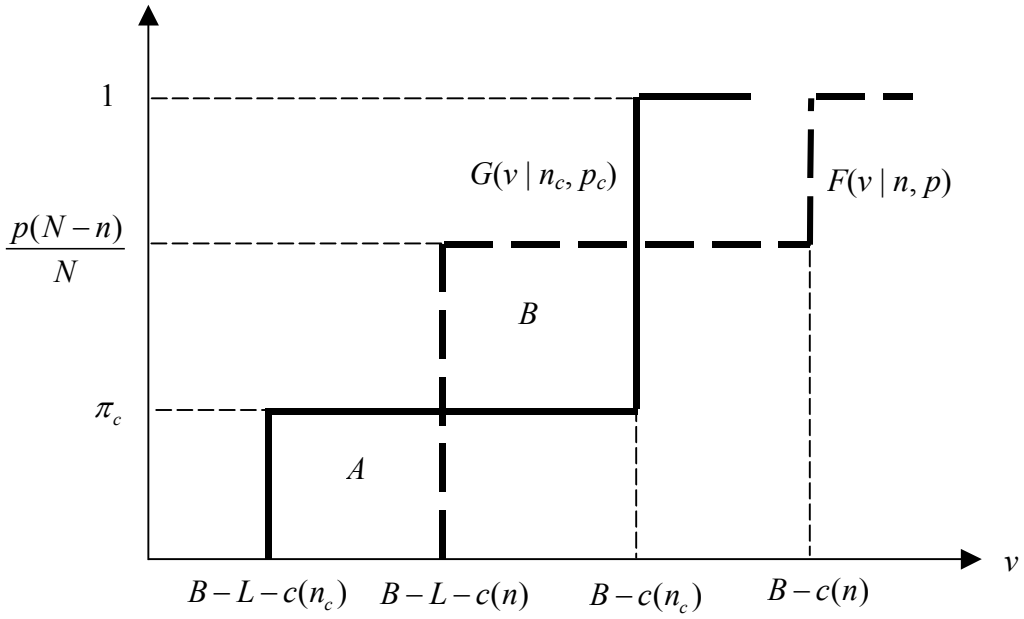

Figure 1: Depiction of the Stochastic Dominance Performance Requirement

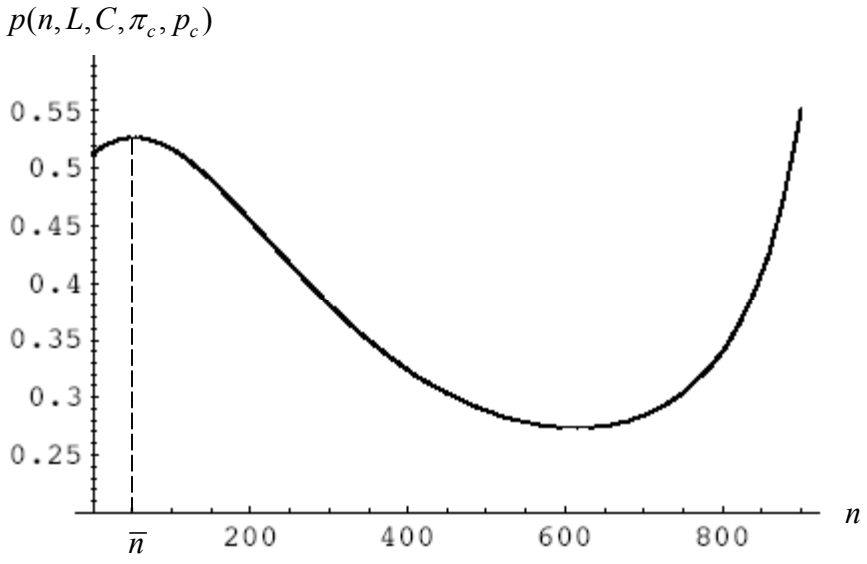

Figure 2: Robustness and Inspections

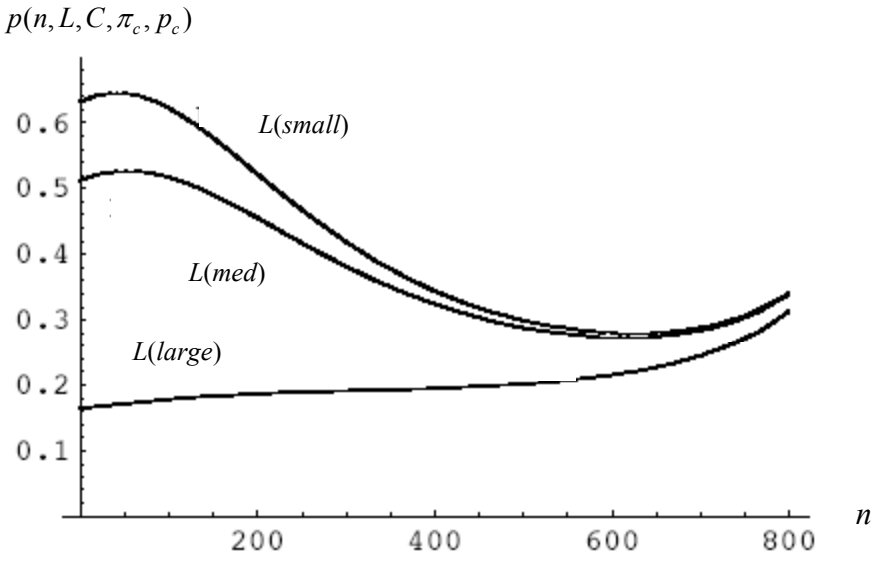

Figure 3: Robustness and the Loss from a Successful Attack.

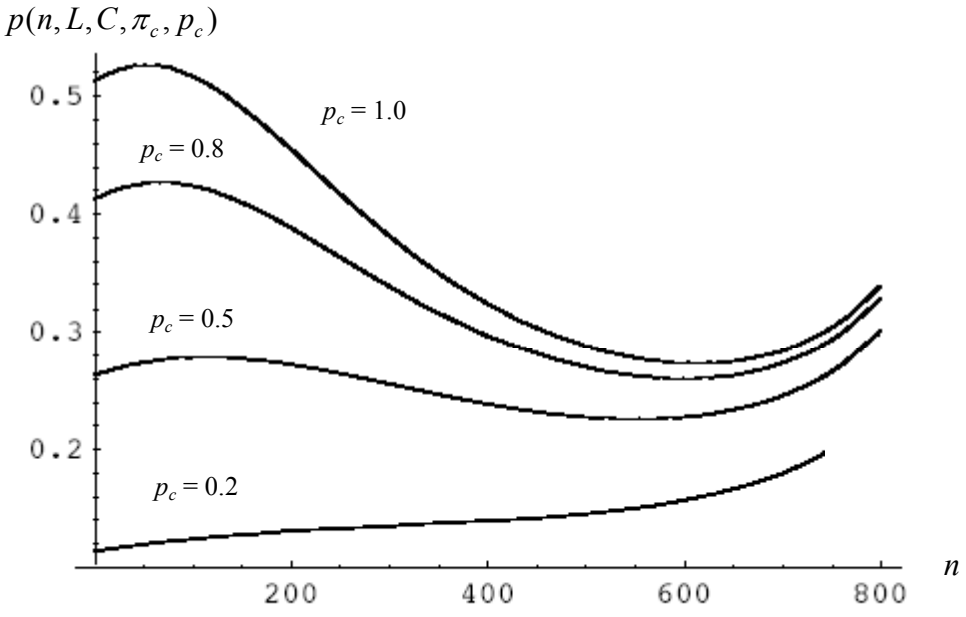

Figure 4: Robustness and the Maximum Probability of an Attack.