Risk, Deterrence, and Prospect Theory: Decision Bias Influence on Quantifiable Deterrence Efficacy in Reducing Risk
By Eric Taquechel
Abstract

Evidence of biased decision-making is well documented. For a practical exercise such as examining efficacy of quantifiable deterrence on CIKR risk reduction and resilience maximization investments, it makes sense to account for such bias. Prospect theory is a well-established theory of biased decision-making based on mounting evidence. Scholars have applied it in numerous contexts but not yet explicitly to the study of the relationship between quantifiable deterrence and risk reduction. This work therefore applies prospect theory and other theories of biased decision-making to advance the study of the relationship between quantifiable deterrence and CIKR risk reduction metrics. Champions of deterrence metrics in the CIKR protection world will be interested to know whether deterrence efficacy is robust to changes in assumptions in how people make decisions. CIKR operators will be interested to know support they receive from government grants to enhance protection efforts is robust to variability in modeling inputs.

Introduction

The study of deterrence is important to critical infrastructure and key resource (CIKR) risk and resilience analysis. Deterrence necessarily entails analysis of how people make decisions. Intent is the component of the probabilistic risk equation that serves as a proxy for adversary decision making. Probabilistic risk has long underpinned critical infrastructure protection efforts; therefore, analyzing intent as a proxy for decision-making supports analysis of deterrence.

Taquechel and Lewis proposed that biases become relevant to CIKR risk reduction when we consider adversarial decision-making. Specifically, prospect theory (PT) predicts, and evidence shows, that people make decisions “nonlinearly.” One PT attribute demonstrating nonlinearity is the framing effect: people make decisions differently based on how options are presented or framed. Therefore, attacker intent may change based on framing. Sensitivity analysis is a process to determine how outputs of a methodology differ in response to variation of the inputs or conditions. When a factor in a risk assessment has uncertainty, sensitivity analysis examines the effect that uncertainty has on the assessment results. Uncertainty is useful in understanding that likelihoods and consequences may not always have a high degree of accuracy or precision. Therefore, adversary decision processes represent uncertainty, but by approximating them with different biased decision-making models, we can conduct sensitivity analysis to estimate the uncertainty.

If theory and evidence suggest people make decisions differently depending on framing effects, the deterrence effects of critical infrastructure protection efforts may be sensitive to variations in framing, creating a range of uncertainty in the outcomes. More specifically, we want to explore implications if we believe deterrence influences the efficacy of CIKR risk reduction investments in specific circumstances, but deterrence is based on biased decision-making. CIKR operators need to understand the range of risk estimate sensitivity and uncertainty to predict how investments may reduce their risk.
If our objective is to reduce risk without considering deterrence effects, we may be able to eliminate uncertainties in adversarial decision-making estimates, specifically by disregarding the influence of biased decision-making. Instead, if our objective is to reduce risk by accounting for deterrence effects, it may be valuable to model how biased decision-making could influence risk reduction when we quantify deterrence and fold it into risk calculations.

Taquechel (2021) studied the effects of deterrence quantification upon risk reduction in several scenarios, including reducing risk of weapon of mass destruction (WMD) transfer through the maritime transportation system, and increasing resilience of a supply chain network after attack on its supplier node. This work showed that accounting for deterrence effects yielded better risk reduction in certain cases, worse risk reduction in other cases, and made no difference in a third set of cases. This work concluded that accounting for quantifiable deterrence efficacy on risk reduction investments might not be universally desirable.

However, Taquechel’s research assumed Expected Utility Theory (EUT) as the basis for utility functions in his deterrence games. He advocated that future research into the relationship between risk reduction and quantifiable deterrence might incorporate principles of PT. Taquechel and Lewis (2016) briefly explored PT and deterrence outside of explicitly proposing whether accounting for quantifiable deterrence resulted in better or worse risk reduction metrics. Their focus was primarily on whether obfuscating security investments from would-be attackers was more advantageous than publicizing such investments, under different assumptions of EUT and PT.

This work focuses intentionally on a very specific application of nonlinear decision making. That said, the larger context for this work is the application of behavioral economics to risk analysis. This larger context extends beyond merely utility theory or prospect theory as the core quantitative models. Behavioral economics entails great complexity, accounting for biases and heuristics that branch out from loss-aversion and variability in calculations of risk.

Research Goals

Given the above, we want to explore the relationship between risk reduction and quantifiable deterrence when we assume PT rather than EUT.

Findings from exploring these relationships may have implications for risk analysts, CIKR protection stakeholders, budget developers, and policymakers. If we can reduce more risk by accounting for effects of deterrence under EUT assumptions, but lose that advantage under PT assumptions, the usefulness of accounting for quantifiable deterrence in CIKR protection investments is questionable. However, a counterargument may be that PT is not a useful framework for assessing deterrence, CIKR risk reduction, and resilience. Such a finding would in no way detract from the overall value of PT to study of decision-making.

Conversely, findings of equally efficacious quantifiable deterrence across assumptions of both EUT and PT would tell a good story for practitioners. It could suggest that in scenarios where we achieve a quantifiable advantage in risk reduction by factoring in deterrence, that advantage is robust to whether EUT or PT is a better framework to represent adversary decision-making.
In addition to increasing CIKR operator confidence, those who model risk, allocate funding and report metrics may rest easy knowing their investments are robust to this type of sensitivity.

Article Organization

The overall organization of this article is as follows. We:
1. Review relevant literature;
2. Introduce the analysis frameworks we will use to elucidate the relationships between risk reduction, deterrence, and biased decision-making theories;
3. Explain each framework’s concept and results of applying the framework using notional data;
4. Summarize framework findings;
5. Offer recommendations for future research; and
6. Offer practical implications of this research and offer concluding remarks.

Literature Review

The literature review will cover three broad categories:
1. Development and evolution of PT;
2. Other proxies for decision-making biases; and
3. Application of PT and other decision-making biases to critical infrastructure risk analysis and deterrence,

Prospect Theory

Original Prospect Theory
Kahneman and Tversky formally introduced PT in 1979 with their seminal work “Prospect Theory: An Analysis of Decision under Risk.” Major concepts from their work include framing effects, reference points (RP), loss aversion, and the certainty effect. Their 1981 paper “The Framing of Decisions and the Psychology of Choice” succinctly presents the concept of nonlinear decision-making:

![Figure 1. A hypothetical value function (Kahneman and Tversky, 1981)](image-url)
The x-axis is gains versus losses and the y-axis is value. Here, people value achieving gains less than avoiding losses. If something is presented as a gain relative to a RP (the intersection of the axes), the utility of that gain increases at a rate slower than does the negative utility of a numerically equal loss.

The concept of loss aversion derives from the steeper slope in the lower left quadrant. People are more likely to take actions to avoid losses than they are to achieve numerically equivalent gains. The certainty effect means people prefer a sure but smaller gain, and the reflection effect inverts that to loss framing: people are willing to risk an uncertain but possibly numerically greater loss rather than a sure but smaller loss. In either frame, people demonstrate loss avoidance.

**Modification – Cumulative Prospect Theory**

Tversky and Kahneman published an advancement in PT, which they called “cumulative prospect theory” (CPT) in 1992. Fennema and Wakker\(^\text{10}\) explain how Tversky and Kahneman’s update addressed theoretical concerns with the original PT, although CPT maintained some original principles of PT including loss aversion and RPs.

Tversky and Kahneman use a value function for CPT:

\[
v(x) = \begin{cases} 
  x^\alpha & \text{if } x \geq 0 \\
  -\lambda(-x)^\beta & \text{if } x < 0 
\end{cases}
\]

**Equation 1.** CPT value function (Tversky and Kahneman, 1992)

Here prospects (x) with numerical value greater than or equal to zero are subject to exponentiation, whereas prospects with numerical value less than zero are subject to both exponentiation and a loss aversion multiplier. This equation uses zero as a normalized RP.\(^\text{11}\) The loss aversion multiplier reflects how the slope of the value function in Figure 1 changes more rapidly in the lower left quadrant (losses) than in the upper right quadrant (gains).

**Biased Decisionmaking—Other Than Prospect Theory**

**Shalev**

Shalev illustrates a “loss-aversion equilibrium” where the expected equilibrium outcome of a game is equal to the player’s RP.\(^\text{12}\) He defines expected utility with loss aversion as follows:
Risk, Deterrence, and Prospect Theory: Decision Bias Influence on Quantifiable Deterrence Efficacy in Reducing Risk | By Eric Taquechel

**Equation 2.** Loss aversion utility (Shalev, 2000)

\[ v_i(x_i, r_i) = \begin{cases} 
  x_i & \text{if } x_i \geq r_i \\
  x_i - \lambda_i(r_i - x_i) & \text{if } x_i < r_i 
\end{cases} \]

Shalev acknowledges the form of this function, while similar to that of the CPT value function from Equation 1, will not exactly pattern after it. However, this function accounts for loss aversion, although not as a function of RP.\textsuperscript{13}

Gains in excess of a RP are not exponentiated, meaning the relationship between numerical value of prospects and their weighted utility is linear. In fact, Shalev does not modify gains at all in this approach, inconsistent with CPT. Shalev also does not exponentiate losses, although they are still subject to a loss aversion factor, albeit a linear one.

**Quijano et al.**

Quijano and colleagues\textsuperscript{14} describe a defender-attacker-defender model where the attacker has incomplete information about defender investments to protect a CIKR network. They model their defender as risk averse, meaning a risk aversion parameter biases their expected utility as a function of investment. Quijano et al. do not explicitly discuss PT or CPT, but their risk aversion parameter serves as a proxy for biased decision-making.

**Application Of Prospect Theory to CIKR Risk and Deterrence**

**Taquechel and Lewis**

Taquechel and Lewis explored how quantification of deterrence might incorporate basic principles of PT.\textsuperscript{15} Unlike some authors who modify expected utility functions based on principles of PT and then calculate game outcomes, Taquechel and Lewis made no changes to expected utility functions when assuming PT.

Instead, they leveraged PT principles of certainty effect and reflection effect to predict what an attacker might prefer. This meant PT applied to the output prospects of game theoretical scenarios, vice the “input prospects” of probabilities and consequences.

Taquechel and Lewis assumed an exogenously given attacker RP of maximum monetized death/injury and total economic losses from destruction of both CIKR targets in a two-target game. This meant any attacker result would be a loss relative to the RP. This exogenous attacker RP was independent of specific permutations of equilibrium outcomes, which contrasts with other authors’ use of endogenous RP.
Taquechel and Lewis stopped short of quantifying deterrence outside of a pure strategy Nash Equilibrium. However, previous work on quantifying deterrence leveraged intent ratios.\textsuperscript{16}

**Merrick and Leclerc**

Merrick and Leclerc\textsuperscript{17} model a container screening game between a defender and an attacker considering smuggling in a radiological dispersal device (RDD) or conventional weapons. Their objective is to explore how assumptions about the attacker decision-making influence deterrence of RDD smuggling, incorporating principles of CPT.

They quantify the “loss aversion threshold” below which an attacker will prefer smuggling conventional weapons rather than an RDD, based on the probability the defender may or may not screen for RDD, and anticipate RDD screening effectiveness if the defender does in fact screen.

Merrick and Leclerc explore an excursion where the defender selects a proportion of containers for screening. They quantify the prescriptive “optimal container screening percentage” based on attacker loss aversion.

This approach assumes imperfect information: the attacker does not know whether the defender is screening or not. However, it plays out both possibilities as separate games to model what an attacker would consider, which should inform defender decisions. This work combines CPT with deterrence analysis but does not explicitly quantify deterrence and incorporate that into risk reduction metrics.

**Metzger and Rieger**

Metzger and Rieger apply CPT to game theoretic scenarios. Their work claims an oversimplified approach to incorporating PT and CPT concepts into game theoretic analysis is to modify probabilities and outcomes via the CPT probability weighting functions and CPT value functions, respectively. One explanation for this oversimplification is that if the players’ RPs are not exogenous, they then become a function of player payoffs.

They conclude that pure strategy Nash equilibria are invariant with respect to value functions and probability weighting functions. However, mixed strategy equilibria are less straightforward; mixed strategy preference distributions are functions of each player’s probability weighting bias and thus create interdependency.

Metzger and Rieger also suggest CPT may not work as well for game theoretical analysis as the original PT might.\textsuperscript{18} Furthermore, they note that probability weighting is less popular than value function analysis in the game theoretic literature.
Summary of Context for Simulations

We now summarize issues from the literature review that provide context for our approach to simulate the effects of CPT upon quantifiable deterrence efficacy on risk reduction.

1. Loss aversion is modeled exponentially in CPT, but some authors have modeled it linearly.
2. RPs are endogenous in existing literature but create theoretical problems.
3. The existing literature accounts for probability weighting less often than for value functions.
4. Efforts to incorporate PT/CPT and other theories of decision-making bias into CIKR risk analysis and deterrence stop short of explicitly exploring how such biases might change the efficacy of quantifiable deterrence on risk reduction metrics.
5. Previous efforts to apply PT to quantification of deterrence were rudimentary and did not explore a gamut of ways to proxy deterrence quantification. These efforts applied PT principles to the outcomes of game theoretic scenarios, not to inputs.

We then summarize findings from Taquechel (2021):

1. Optimize for Vulnerability - When we optimize vulnerability reduction investment to minimize risk of a WMD shipped through the maritime transportation system, accounting for quantifiable deterrence effects using attacker intent ratios made no difference on total risk reduction. Moreover, under one specific set of assumptions about attacker decision-making, accounting for quantifiable deterrence achieved less risk reduction than disregarding effects of deterrence.

   However, assuming CPT instead of EUT might yield that accounting for quantifiable deterrence leads to improved risk reduction metrics.

2. Optimize for Consequence – The relative efficacy of quantifiable deterrence in increasing network resilience is greater than when we disregard the effects of deterrence in a simulation of notional supply chain networks. However, assuming CPT instead of EUT might yield that accounting for quantifiable deterrence leads to less resilience maximization. That said, for brevity of exposition the following analysis will focus on vulnerability reduction alone.

CPT And Deterrence Simulations: Concepts of Operation and Results

Baseline - No Deterrence vs Deterrence (Intent Ratio), EUT

Taquechel (2021) enumerated conditional risk results of optimizing WMD detection equipment investment to reduce transfer risk, across a variety of attacker pathways. A pathway was a specific combination of foreign ports and domestic U.S. ports an attacker could exploit to ship a WMD.
He then enumerated unconditional risk results of optimizing detection equipment investment across the same pathways, using intent ratio as a proxy for quantifiable deterrence effects. As compared to the results without deterrence, factoring in intent ratio as a proxy for quantified deterrence made no difference in overall risk reduction metrics.

Now we explore whether CPT influences the relationship between risk reduction and deterrence when we optimize for vulnerability in various simulations. To narrow focus on the effects of EUT vs CPT alone, these simulations use the same notional transfer network fault tree model and data from Taquechel (2021).

**Simulation 1 – Deterrence – Intent Ratios – Cumulative Prospect Theory – All Losses**

Here we apply Tversky and Kahneman’s CPT to intent ratios. We assume an exogenously given attacker RP equal to the maximum consequence of both targets, here $4 million, so any probabilistic expectation will be less than the RP and therefore loss aversion functions apply to all attacker prospects.

To apply CPT, we revisit the pathway expected utility (UeT) for each attacker pathway course of action (COA) and calculate the difference from the RP. In CPT, changes from the RP, not changes in net asset position, are carriers of wealth.

<table>
<thead>
<tr>
<th>COA</th>
<th>UeT</th>
<th>Delta UeT and RP</th>
</tr>
</thead>
<tbody>
<tr>
<td>COA 7: AND-AND</td>
<td>$82,396.08</td>
<td>$3,917,603.92</td>
</tr>
<tr>
<td>COA 4: AND-OR, Exploit DP2</td>
<td>$138,264.06</td>
<td>$3,861,735.94</td>
</tr>
<tr>
<td>COA 3: AND-OR, Exploit DP1</td>
<td>$148,983.18</td>
<td>$3,851,016.82</td>
</tr>
<tr>
<td>COA 5: OR-AND, exploit FP 1</td>
<td>$329,584.31</td>
<td>$3,670,415.69</td>
</tr>
<tr>
<td>COA 6: OR-AND, exploit FP 2</td>
<td>$329,584.31</td>
<td>$3,670,415.69</td>
</tr>
<tr>
<td>COA 2: OR-OR, Exploit DP2</td>
<td>$967,848.40</td>
<td>$3,032,151.60</td>
</tr>
<tr>
<td>COA 1: OR-OR, Exploit DP1</td>
<td>$1,042,882.29</td>
<td>$2,957,117.71</td>
</tr>
</tbody>
</table>

These COAs are ordered from least to greatest UeT. The greater the expected utility, the smaller the difference from the RP.

We next apply the CPT value function to the delta in expected utility from the RP.

The delta is “x” in the piecewise equation. Since prospects are losses in this example, we use only the second part of the piecewise equation. The data is:
Table 2 Attacker expected utility and CPT Value Function

<table>
<thead>
<tr>
<th>COA</th>
<th>UeT</th>
<th>CPT Value Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>COA 7: AND-AND</td>
<td>$82,396.08</td>
<td>$(1,425,740.81)</td>
</tr>
<tr>
<td>COA 4: AND-OR, Exploit DP2</td>
<td>$138,264.06</td>
<td>$(1,407,833.14)</td>
</tr>
<tr>
<td>COA 3: AND-OR, Exploit DP1</td>
<td>$148,983.18</td>
<td>$(1,404,393.73)</td>
</tr>
<tr>
<td>COA 5: OR-AND, exploit FP 1</td>
<td>$329,584.31</td>
<td>$(1,346,269.29)</td>
</tr>
<tr>
<td>COA 6: OR-AND, exploit FP 2</td>
<td>$329,584.31</td>
<td>$(1,346,269.29)</td>
</tr>
<tr>
<td>COA 2: OR-OR, Exploit DP2</td>
<td>$967,848.40</td>
<td>$(1,137,950.36)</td>
</tr>
<tr>
<td>COA 1: OR-OR, Exploit DP1</td>
<td>$1,042,882.29</td>
<td>$(1,113,132.59)</td>
</tr>
</tbody>
</table>

The smaller the delta, the less negative the value function is, or the closer the COA’s utility to the RP. The negative data denotes loss relative to the RP.

We now leverage the value function to create intent ratios, reflecting attacker relative preferences for different COAs. First, we evaluate percentage of CPT value function variation from the RP to proxy “closeness” to the RP.

Table 3: Value Function and CPT Closeness to RP

<table>
<thead>
<tr>
<th>COA</th>
<th>CPT Value Function</th>
<th>Closeness to RP</th>
</tr>
</thead>
<tbody>
<tr>
<td>COA 7: AND-AND</td>
<td>$(1,425,740.81)</td>
<td>0.64</td>
</tr>
<tr>
<td>COA 4: AND-OR, Exploit DP2</td>
<td>$(1,407,833.14)</td>
<td>0.65</td>
</tr>
<tr>
<td>COA 3: AND-OR, Exploit DP1</td>
<td>$(1,404,393.73)</td>
<td>0.65</td>
</tr>
<tr>
<td>COA 5: OR-AND, exploit FP 1</td>
<td>$(1,346,269.29)</td>
<td>0.66</td>
</tr>
<tr>
<td>COA 6: OR-AND, exploit FP 2</td>
<td>$(1,346,269.29)</td>
<td>0.66</td>
</tr>
<tr>
<td>COA 2: OR-OR, Exploit DP2</td>
<td>$(1,137,950.36)</td>
<td>0.72</td>
</tr>
<tr>
<td>COA 1: OR-OR, Exploit DP1</td>
<td>$(1,113,132.59)</td>
<td>0.72</td>
</tr>
</tbody>
</table>

The larger (here less negative) the CPT value function, the closer it is to the RP. Finally, we convert closeness to an intent ratio by dividing closeness of each COA by aggregate closeness.

Table 4: Closeness to RP and CPT Intent Ratio

<table>
<thead>
<tr>
<th>COA</th>
<th>Closeness to RP</th>
<th>CPT Intent Ratio</th>
</tr>
</thead>
<tbody>
<tr>
<td>COA 1: OR-OR, Exploit DP1</td>
<td>0.72</td>
<td>0.153</td>
</tr>
<tr>
<td>COA 2: OR-OR, Exploit DP2</td>
<td>0.72</td>
<td>0.152</td>
</tr>
<tr>
<td>COA 3: AND-OR, Exploit DP1</td>
<td>0.65</td>
<td>0.138</td>
</tr>
<tr>
<td>COA 4: AND-OR, Exploit DP2</td>
<td>0.65</td>
<td>0.138</td>
</tr>
<tr>
<td>COA 5: OR-AND, exploit FP 1</td>
<td>0.66</td>
<td>0.141</td>
</tr>
<tr>
<td>COA 6: OR-AND, exploit FP 2</td>
<td>0.66</td>
<td>0.141</td>
</tr>
<tr>
<td>COA 7: AND-AND</td>
<td>0.64</td>
<td>0.137</td>
</tr>
</tbody>
</table>

This table changes the order of data entries to reflect the sequence of COAs. We expand the CPT intent ratio to three decimal places to differentiate.

To maximize context for these results we add the original attacker expected utilities of each COA from Table 1 back in:
Risk, Deterrence, and Prospect Theory: Decision Bias Influence on Quantifiable Deterrence Efficacy in Reducing Risk | By Eric Tauechel

Table 5: COA, UeT and CPT Intent Ratio

<table>
<thead>
<tr>
<th>COA</th>
<th>UeT</th>
<th>CPT Intent Ratio</th>
</tr>
</thead>
<tbody>
<tr>
<td>COA 1: OR-OR, Exploit DP1</td>
<td>$1,042,882.29</td>
<td>0.153</td>
</tr>
<tr>
<td>COA 2: OR-OR, Exploit DP2</td>
<td>$967,848.40</td>
<td>0.152</td>
</tr>
<tr>
<td>COA 3: AND-OR, Exploit DP1</td>
<td>$148,983.18</td>
<td>0.138</td>
</tr>
<tr>
<td>COA 4: AND-OR, Exploit DP2</td>
<td>$138,264.06</td>
<td>0.138</td>
</tr>
<tr>
<td>COA 5: OR-AND, exploit FP 1</td>
<td>$329,584.31</td>
<td>0.141</td>
</tr>
<tr>
<td>COA 6: OR-AND, exploit FP 2</td>
<td>$329,584.31</td>
<td>0.141</td>
</tr>
<tr>
<td>COA 7: AND-AND</td>
<td>$82,396.08</td>
<td>0.137</td>
</tr>
</tbody>
</table>

Therefore, we may predict that under CPT assumptions the attacker prefers COA 1 as a priority, followed by COA 2, followed by indifference between COAs 5 and 6, followed by indifference between COAs 3 and 4, followed by COA 7. This is not necessarily a different preference ordering than when we assume EUT, but the relative strength of the preferences may change.\(^{21}\)

With that in mind, we compare these intent ratios to those assuming EUT:

Table 6: COA, UeT and EUT Intent Ratio

<table>
<thead>
<tr>
<th>COA</th>
<th>UeT</th>
<th>EUT Intent Ratio</th>
</tr>
</thead>
<tbody>
<tr>
<td>COA 1: OR-OR, Exploit DP1</td>
<td>$1,042,882.29</td>
<td>0.343</td>
</tr>
<tr>
<td>COA 2: OR-OR, Exploit DP2</td>
<td>$967,848.40</td>
<td>0.318</td>
</tr>
<tr>
<td>COA 3: AND-OR, Exploit DP1</td>
<td>$148,983.18</td>
<td>0.049</td>
</tr>
<tr>
<td>COA 4: AND-OR, Exploit DP2</td>
<td>$138,264.06</td>
<td>0.045</td>
</tr>
<tr>
<td>COA 5: OR-AND, exploit FP 1</td>
<td>$329,584.31</td>
<td>0.108</td>
</tr>
<tr>
<td>COA 6: OR-AND, exploit FP 2</td>
<td>$329,584.31</td>
<td>0.108</td>
</tr>
<tr>
<td>COA 7: AND-AND</td>
<td>$82,396.08</td>
<td>0.027</td>
</tr>
</tbody>
</table>

We make two observations. First, the highest utility COAs are preferred more strongly (relative to other COAs) under EUT assumptions than they are under CPT assumptions (.343 vs .153). Second, the range of variation in intent ratio is greater under EUT assumptions than under CPT assumptions. We demonstrate this graphically, first with EUT intent ratios.
Here we see an exponential best-fit change in desirability of outcomes as the expected utility grows. The x-axis represents “steps” of increase in net asset position rather than the numerical expected utilities of increasing net asset position, for scaling purposes. The y-axis is the intent ratio representing the desirability of different outcomes. The expected utility in this example, coincidentally, also grows exponentially so we must interpret this preference data cautiously, especially since such growth is inconsistent with EUT’s diminishing marginal utility theory.

Next, we show CPT intent ratios:

**Figure 2.** Change in Intent Ratio as Net Asset Positions Increase, EUT

**Figure 3.** Change in Intent Ratio as Net Asset Positions Increase, CPT, All Losses
Here we see a polynomial best fit. The axes are the same as in the previous figure.

It is difficult to compare best fits and changes in slope. We can show nonlinear intent ratio increase with expected utility increase when we assume CPT, as opposed to linear intent ratio increase for same expected utility increases when we assume EUT.23

However, different slope might be more salient if we compared intent ratios for CPT results when expected outcomes are all gains, or a mix of gains and losses relative to a RP. In fact, Tversky and Kahneman used different equations for when all prospects are gains or when prospects are losses,24 as opposed to a prospect containing both gains and losses, so use of their 1992 parameters to estimate loss aversion in this research may not be theoretically consistent with their work. That said, Tversky and Kahneman did not elicit preferences in a noncooperative context, so the importance of theoretical consistency is unknown at this time.

The foregoing explains how to apply CPT principles to attacker preferences. Now, we need to focus on operational concerns. We now evaluate risk implications of these intent ratios for the defender.

<table>
<thead>
<tr>
<th>ALLOCATION DP1</th>
<th>ALLOCATION DP2</th>
<th>RESULTING UNCONDITIONAL RISK (COA 1)</th>
<th>ALLOCATION TACTIC</th>
<th>% RISK REDUX</th>
</tr>
</thead>
<tbody>
<tr>
<td>$0</td>
<td>$0</td>
<td>$204,879.58</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>$839,035.95</td>
<td>$1,160,964.05</td>
<td>$173,124.39</td>
<td>MAX DP2</td>
<td>15.50%</td>
</tr>
<tr>
<td>$1,000,000.00</td>
<td>$1,000,000.00</td>
<td>$168,709.31</td>
<td>EVEN SPLIT</td>
<td>17.65%</td>
</tr>
<tr>
<td>$2,000,000.00</td>
<td>$0</td>
<td>$149,667.94</td>
<td>MAX DP1</td>
<td>26.95%</td>
</tr>
</tbody>
</table>

To compare, we show the results when we assumed EUT:

<table>
<thead>
<tr>
<th>ALLOCATION DP1</th>
<th>ALLOCATION DP2</th>
<th>RESULTING UNCONDITIONAL RISK (COA 1)</th>
<th>ALLOCATION TACTIC</th>
<th>% RISK REDUX</th>
</tr>
</thead>
<tbody>
<tr>
<td>$0</td>
<td>$0</td>
<td>$459,056.21</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>$839,035.95</td>
<td>$1,160,964.05</td>
<td>$391,577.55</td>
<td>MAX DP2</td>
<td>14.70%</td>
</tr>
<tr>
<td>$1,000,000.00</td>
<td>$1,000,000.00</td>
<td>$344,292.16</td>
<td>EVEN SPLIT</td>
<td>16.67%</td>
</tr>
<tr>
<td>$2,000,000.00</td>
<td>$0</td>
<td>$344,292.16</td>
<td>MAX DP1</td>
<td>25.00%</td>
</tr>
</tbody>
</table>

We see that the initial CPT unconditional risk (no allocation) is less because the intent ratio for COA 1 is less under assumptions of CPT than under EUT assumptions. Moreover, we see relatively more risk reduction from optimal investment under CPT assumptions (26.95%) than under EUT assumptions (25%), as seen in the column “% risk redux.”

This comparison suggests deterrence is more meaningful to risk reduction when we assume CPT than when we assume EUT, assuming all attacker prospects are losses relative to a RP and given this particular WMD transfer risk scenario and data.
We show the results when we assumed no quantifiable deterrence, resulting in conditional risk:

<table>
<thead>
<tr>
<th>ALLOCATION DP1</th>
<th>ALLOCATION DP2</th>
<th>RESULTING CONDITIONAL RISK (COA 1)</th>
<th>ALLOCATION TACTIC</th>
<th>% RISK REDUX</th>
</tr>
</thead>
<tbody>
<tr>
<td>$0</td>
<td>$0</td>
<td>$1,312,500.00</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>$839,035.95</td>
<td>$1,160,964.05</td>
<td>$1,119,569.94</td>
<td>MAX DP2</td>
<td>14.70%</td>
</tr>
<tr>
<td>$1,000,000.00</td>
<td>$1,000,000.00</td>
<td>$1,093,750.00</td>
<td>EVEN SPLIT</td>
<td>16.67%</td>
</tr>
<tr>
<td>$2,000,000.00</td>
<td>$0</td>
<td>$984,375.00</td>
<td>MAX DP1</td>
<td>25.00%</td>
</tr>
</tbody>
</table>

This is encouraging for those who advocate deterrence in CIKR risk reduction. A government agency charged with allocating investments to improve security may rest easy knowing the investments are more effective when we account for decision bias, as PT has proven. However, we must first explore the results of other attacker COAs. Consistent with the category of this simulation, we note that any conclusions must keep in mind the relationship between attacker COA outcomes and their RP—in this simulation, all losses.

Detailed analysis of the other attacker COAs is available from the author.

Summary – Simulation 1

After analysis of the other COAs, we can see that in only two of six instances does accounting for quantifiable deterrence under CPT assumptions provide any advantage over quantifiable deterrence under EUT assumptions, or without accounting for deterrence in the first place. This reverses the findings from COA 1 and thus is not encouraging for those who would advocate incorporation of quantifiable deterrence effects into risk reduction analysis.

Simulation 2 – Deterrence – Intent Ratios – Cumulative Prospect Theory – Mix Losses and Gains

What if the attacker’s RP changes? We set the attacker’s RP to $200K to enable a generally equal distribution of gains vs losses in the seven COA outcomes.

We then modify expected utilities that are gains relative to this new RP per Tversky and Kahneman but leave the expected utility modification from the previous simulation the same for losses. We use the same logic for calculating “RP closeness” and resulting intent ratios.

We now evaluate the risk implications for the defender.
Table 10: Defender Unconditional Risk from Attacker COA 1, Intent Ratios, CPT, Mix Gains and Losses

<table>
<thead>
<tr>
<th>ALLOCATION DP1</th>
<th>ALLOCATION DP2</th>
<th>RESULTING UNCONDITIONAL RISK (COA 1)</th>
<th>ALLOCATION TACTIC</th>
<th>% RISK REDUX</th>
</tr>
</thead>
<tbody>
<tr>
<td>$0</td>
<td>$0</td>
<td>$295,555.26</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>$839,035.95</td>
<td>$1,160,964.05</td>
<td>$255,034.96</td>
<td>MAX DP2</td>
<td>13.71%</td>
</tr>
<tr>
<td>$1,000,000.00</td>
<td>$1,000,000.00</td>
<td>$247,124.80</td>
<td>EVEN SPLIT</td>
<td>16.39%</td>
</tr>
<tr>
<td>$2,000,000.00</td>
<td>$0</td>
<td>$208,169.12</td>
<td>MAX DP1</td>
<td>29.57%</td>
</tr>
</tbody>
</table>

We again show the results when we assumed EUT:

Table 11: Defender Unconditional Risk from Attacker COA 1, Intent Ratios, EUT (Taquechel, 2021)

<table>
<thead>
<tr>
<th>ALLOCATION DP1</th>
<th>ALLOCATION DP2</th>
<th>RESULTING UNCONDITIONAL RISK (COA 1)</th>
<th>ALLOCATION TACTIC</th>
<th>% RISK REDUX</th>
</tr>
</thead>
<tbody>
<tr>
<td>$0</td>
<td>$0</td>
<td>$459,056.21</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>$839,035.95</td>
<td>$1,160,964.05</td>
<td>$391,577.55</td>
<td>MAX DP2</td>
<td>14.70%</td>
</tr>
<tr>
<td>$1,000,000.00</td>
<td>$1,000,000.00</td>
<td>$382,546.84</td>
<td>EVEN SPLIT</td>
<td>16.67%</td>
</tr>
<tr>
<td>$2,000,000.00</td>
<td>$0</td>
<td>$344,292.16</td>
<td>MAX DP1</td>
<td>25.00%</td>
</tr>
</tbody>
</table>

As with the simulation where all outcomes are losses, here we see relatively more risk reduction under CPT assumptions (29.57%) than under EUT assumptions (25%), when we account for quantifiable deterrence.

We again show the results when we assumed no quantifiable deterrence, resulting in conditional risk:

Table 12: Defender Conditional Risk from Attacker COA 1 (Taquechel, 2021)

<table>
<thead>
<tr>
<th>ALLOCATION DP1</th>
<th>ALLOCATION DP2</th>
<th>RESULTING CONDITIONAL RISK (COA 1)</th>
<th>ALLOCATION TACTIC</th>
<th>% RISK REDUX</th>
</tr>
</thead>
<tbody>
<tr>
<td>$0</td>
<td>$0</td>
<td>$1,312,500.00</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>$839,035.95</td>
<td>$1,160,964.05</td>
<td>$1,119,569.94</td>
<td>MAX DP2</td>
<td>14.70%</td>
</tr>
<tr>
<td>$1,000,000.00</td>
<td>$1,000,000.00</td>
<td>$1,093,750.00</td>
<td>EVEN SPLIT</td>
<td>16.67%</td>
</tr>
<tr>
<td>$2,000,000.00</td>
<td>$0</td>
<td>$984,375.00</td>
<td>MAX DP1</td>
<td>25.00%</td>
</tr>
</tbody>
</table>

Therefore, we again can claim accounting for quantifiable deterrence provides value, since we can reduce more risk by accounting for intent ratios under CPT assumptions, than we can absent deterrence.

This continues to be encouraging for those who advocate quantifiable deterrence in CIKR risk reduction. However, we must temper this enthusiasm with exploration of the other attacker COAs. Exploiting a supply chain to transfer illicit materials can offer many routes between origin and destination to an adversary. Detailed analysis of the other attacker COAs is available from the author.
Summary– Simulation 2

We compare findings to those of Simulation 1.

- For COA 1, accounting for quantifiable deterrence under CPT assumptions where outcomes were a mix of losses and gains provided value, as compared to accounting for deterrence under EUT assumptions, and as compared to disregarding deterrence. This held when we assumed all losses. This tells a good story for advocates of quantifiable deterrence and for advocates of accounting for PT, who may find satisfactory this evidence that if the attacker chooses COA 1, quantifiable deterrence efficacy is consistent across variations in attacker reference point.

- For COA 2, accounting for quantifiable deterrence under CPT assumptions where outcomes were a mix of losses and gains provided no value, as compared to accounting for deterrence under EUT assumptions, and as compared to disregarding deterrence. However, it did provide value for all losses. This paints a slightly less rosy picture for those who might advocate both quantifiable deterrence and PT, since quantifiable deterrence efficacy was brittle to changes in attacker RP.

- For COA 3, accounting for quantifiable deterrence under CPT assumptions where outcomes were a mix of losses and gains provided value, as compared to accounting for deterrence under EUT assumptions and disregarding deterrence. However, this is inconsistent with findings under assumptions of all losses, where deterrence provided no value. This further supports the claim that quantifiable deterrence efficacy is brittle to changes in attacker RP.

- For COA 4, accounting for quantifiable deterrence under CPT assumptions where outcomes were a mix of losses and gains provided no value. This is consistent with findings under assumptions of all losses, and thus would be satisfying to detractors of quantifiable deterrence.

- For COA 5, we see that accounting for quantifiable deterrence provides no value for either EUT or CPT assumptions. This also held for assumptions of all losses. This robustness confirms limited value of deterrence quantification advocacy, although practitioners may be satisfied to know that changing analysis assumptions yielded consistent risk reduction results for this particular attacker COA. A practitioner may be indifferent to nuances of deterrence theory but may rightly be more concerned with the robustness of investments to defend their infrastructure or minimize chance of exploitation.

- For COA 6, accounting for quantifiable deterrence under CPT assumptions provided value, as compared to accounting for deterrence under EUT assumptions and disregarding deterrence. This did not hold when we assumed all losses. This further supports the claim that quantifiable deterrence efficacy is brittle to changes in attacker RP.
These findings of quantifiable deterrence efficacy brittleness to attacker RP changes, and consistent inefficacy of quantifiable deterrence in reducing risk across multiple RPs in specific cases, are not especially encouraging for those who would advocate incorporation of quantifiable deterrence effects into risk reduction analysis under the assumption of CPT biased decision-making. For only one COA (COA 1) was deterrence efficacy robust across variation in attacker RPs.

Simulation 3 – Deterrence – Intent Ratios – Cumulative Prospect Theory – All Gains

We change the attacker’s RP to $75K to ensure all outcomes are gains. We update the value function equations to eliminate any piecewise functions for losses and recalculate intent ratios using previous logic.

We now evaluate risk implications for the defender.

Table 13: Defender Unconditional Risk from Attacker COA 1, Intent Ratios, CPT, All Gains

<table>
<thead>
<tr>
<th>ALLOCATION DP1</th>
<th>ALLOCATION DP2</th>
<th>RESULTING UNCONDITIONAL RISK (COA 1)</th>
<th>ALLOCATION TACTIC</th>
<th>% RISK REDUX</th>
</tr>
</thead>
<tbody>
<tr>
<td>$0</td>
<td>$0</td>
<td>$339,975.46</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>$839,035.95</td>
<td>$1,160,964.05</td>
<td>$292,816.69</td>
<td>MAX DP2</td>
<td>13.87%</td>
</tr>
<tr>
<td>$1,000,000.00</td>
<td>$1,000,000.00</td>
<td>$282,819.23</td>
<td>EVEN SPLIT</td>
<td>16.81%</td>
</tr>
<tr>
<td>$2,000,000.00</td>
<td>$0</td>
<td>$232,557.20</td>
<td>MAX DP1</td>
<td>31.60%</td>
</tr>
</tbody>
</table>

We jump directly to the results when we assumed no quantifiable deterrence, resulting in conditional risk:

Table 14: Defender Conditional Risk from Attacker COA 1 (Taquechel, 2021)

<table>
<thead>
<tr>
<th>ALLOCATION DP1</th>
<th>ALLOCATION DP2</th>
<th>RESULTING CONDITIONAL RISK (COA 1)</th>
<th>ALLOCATION TACTIC</th>
<th>% RISK REDUX</th>
</tr>
</thead>
<tbody>
<tr>
<td>$0</td>
<td>$0</td>
<td>$1,312,500.00</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>$839,035.95</td>
<td>$1,160,964.05</td>
<td>$1,119,569.94</td>
<td>MAX DP2</td>
<td>14.70%</td>
</tr>
<tr>
<td>$1,000,000.00</td>
<td>$1,000,000.00</td>
<td>$1,093,750.00</td>
<td>EVEN SPLIT</td>
<td>16.67%</td>
</tr>
<tr>
<td>$2,000,000.00</td>
<td>$0</td>
<td>$984,375.00</td>
<td>MAX DP1</td>
<td>25.00%</td>
</tr>
</tbody>
</table>

Therefore, we again can claim accounting for quantifiable deterrence provides value, since we reduce more risk by accounting for intent ratios under CPT assumptions, than we do absent deterrence, this time assuming all gains.

Detailed analysis of the other attacker COAs is available from the author.
Summary – Simulation – 3

For all gains, in only two of six COAs does accounting for quantifiable deterrence present any advantage.

Summary – Optimizing for Vulnerability – Deterrence – Intent Ratios

After evaluating efficacy of quantifiable deterrence under CPT assumptions, for WMD transfer scenarios in which attacker outcomes are all losses, all gains, or a mix relative to a RP, we see that only in limited circumstances is quantifiable deterrence efficacious in improving risk reduction metrics. This is not encouraging for those who would advocate incorporation of quantifiable deterrence effects into risk reduction analysis.

Recommendations For Future Research

Most recommendations for future research from Taquechel (2021) focus on exploring the relationship between deterrence and risk reduction hold here, since the present research specifically focused on biased decision-making. We also addressed the suggestion to explore the implications of suboptimal investment in specific cases.

With that in mind, we offer additional recommendations that follow from the present research.

Linear or Exponential Decision Bias

There is no guarantee CPT is the best theory for modeling biased decision-making in the study of CIKR risk and deterrence. Shalev’s approach to loss averse mixed strategy equilibria leverages a linear loss aversion function, which is inconsistent with CPT. This means intent ratios may not change more for nonlinear decision making than they will for linear decision-making, which may be unsatisfying from a theoretical perspective.

Furthermore, Shalev did not modify gains, which again is inconsistent with CPT. However, exploring the relationship between quantifiable deterrence and risk reduction with linear loss aversion functions in more detail than presented here is an opportunity for future research.

Probability Weighting Functions

This research did not incorporate probability-weighting functions. We assumed attackers considered outcomes as the product of unweighted network exploitation probabilities and consequences of successful WMD transfer, and then we applied the CPT value function to those outcomes to derive intent ratios. This approach therefore modeled loss aversion but without the explicit probability-weighting effects Tversky and Kahneman observed.
If future work on deterrence quantification under assumptions of CPT incorporates probability weighting but yields the same results, the theoretical inconsistency may have no impact on the implications for practitioners.

**Consistency of “Optimal Investment” Efficacy on Risk Reduction**

As we have shown in one example, the definition of optimal investment may not hold under specific circumstances when we analyze quantifiable deterrence under assumptions of biased decision-making. More research might determine when else this applies.

**Modeling Resilience**

Taquechel (2021) explored resilience modeling as well as vulnerability mitigation. Since the government’s mission is to maximize resilience in addition to minimizing risk, future work should explore the relationship between CPT, quantifiable deterrence, and resilience enhancement investments. Quantifiable deterrence efficacy in Taquechel (2021) when optimizing for consequence may or may not hold under CPT assumptions. Initial exploration into this topic has yielded interesting insights on the use of game theory and mixed strategy equilibria applicability to modeling deterrence quantification under CPT conditions.

**Practical Implications**

We have shown that when we assume CPT models biased attacker decision-making, accounting for quantifiable deterrence more often than not adds no value to risk reduction efforts when we optimize investments to minimize transfer network risk.

Challenges discovered were that quantifiable deterrence efficacy was brittle to changes in attacker RP, or it is consistently inefficacious across multiple RPs. If these findings were generalizable across variations in all the modeling assumptions used here, those advocating quantifiable deterrence for risk reduction metrics might be disheartened. Fortunately, for simplicity of exposition, we have explored a limited set of scenarios and there is no guarantee these findings would hold across a larger dataset.

The burden of proof may be on those who advocate the importance of measuring deterrence to show it consistently adds value to risk reduction metrics, when it comes to effort to minimize vulnerability to WMD transfer.

Such burden diminishes neither the theoretical importance of deterring our adversaries nor the importance of modeling biased decision-making. Instead, it increases the importance: future analysis must produce data showing how quantifiable deterrence will reduce transfer risk across a swath of assumptions, to increase value as a reportable metric.
Conclusion

Robust countermeasures can serve as a deterrent to some adversaries, causing them to change, delay or abandon their plans. Here, we explored whether the relationship between risk reduction and deterrence is robust to different assumptions about how adversaries perceive their options, proxied by EUT and CPT, and how they prioritize their options, leveraging intent ratios as proxies for quantifiable deterrence. We cannot claim robustness at this point and maintain limited value of quantifiable deterrence in CIKR risk analysis, but more research is needed.


This research responds to all of these urgings and advances previous work on deterrence quantification and its influence on risk reduction. It explores intent ratios under assumptions of biased decision-making including Shalev’s loss aversion equilibrium and principles from Tversky and Kahneman’s CPT. It proposes a method to calculate attacker intent based on CPT principles and applies that method to evaluate efficacy of quantifiable deterrence to CIKR risk reduction metrics.

The permutations of modeling assumptions, notional data, proxies for quantifiable deterrence, proxies for biased decision-making, and proxies for specific preferences (i.e., RPs) suggest more research is necessary to generalize findings. One long term objective may be to produce a model that will help us conclude, for example, “if attacker RP is X, we can predict efficacy of quantifiable deterrence in improving risk reduction metrics under conditions Y and Z.”

That said, it might not be desirable to focus on predictive models when we are dealing with human decision-making. Therefore, the true value of this research is both advancing previous research and increasing practitioner awareness of the sensitivity of risk reduction analysis to variation in inputs. The variation in inputs here is uncertainty as to attacker perception and prioritization possibilities.

Tversky and Kahneman and did not explicitly derive CPT preference functions in noncooperative or game theoretical contexts, so the importance of this research’s theoretical consistency with Tversky and Kahneman’s methodology is unknown at this time. Efforts to apply their principles to game theoretical contexts are rigorous and insightful, but do not explicitly quantify deterrence and incorporate its effects into risk reduction metrics, a practitioner equity.
About the Author

Eric F. Taquechel is a retired U.S. Coast Guard officer with experience in port operations, critical infrastructure protection and risk analysis, emergency management, operations analysis, strategy/budgeting process support, and international port security management. He has authored and co-authored various publications on risk, resilience, deterrence, and performance metrics in HSAJ, the Journal of Homeland Security and Emergency Management, and IEEE. His paper “A Right-Brained Approach to Critical Infrastructure Protection Theory in support of Strategy and Education: Deterrence, Networks, and Antifragility” was a Best Paper presented at the CHDS’s 2017 10th Annual Homeland Defense and Security Education Summit. Taquechel has taught courses on critical infrastructure protection and is a FEMA Master Exercise Practitioner. He holds a MPA from Old Dominion University, a master’s degree in Security Studies from the Naval Postgraduate School, a graduate certificate in Countering Weapons of Mass Destruction from Missouri State University, and a BS from the U.S. Coast Guard Academy. He may be reached at eric.taquechel@gmail.com.

Acknowledgements

The author thanks the referees who helped improve the quality of this work.

Disclaimer

The original opinions and recommendations in this work are those of the author and are not intended to represent the policies or positions of any government agency or private company.

Bibliography


---

**Glossary**

Critical Infrastructure and Key Resources (CIKR) - systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters

Expected Utility Theory (EUT) - a theory that assumes people find the best possible solution from among all known options, choosing a solution that will maximize their expected utility. They act according to their preferences, and preferences are consistent regardless of how options are presented

Prospect Theory (PT) - an alternative theory of utility which has shown experimentally that decisions made may be inconsistent with EUT, depending on how options are presented or framed

Reference Point (RP) – If something is presented as a gain relative to a RP (the intersection of the axes), the expected utility of that gain increases at a rate slower than does the negative expected utility of a numerically equal loss
Cumulative Prospect Theory (CPT) – expands on the original Prospect Theory by updating the modifier values for gains and losses

PT Value Function – a graph that shows the relationship between utility of a prospect, losses, and gains relative to a reference point

Loss Aversion - a multiplier reflecting how the slope of the PT value function changes more rapidly in the lower left quadrant (losses) than in the upper right quadrant (gains)

Intent Ratio – used as proxy for COA desirability and quantifiable deterrence. When assuming EUT, the ratio of expected utility of one course of action (COA) to combined expected utilities of all COAs under review. When assuming PT, ratio of one COA’s closeness to a reference point, relative to aggregate closeness of all COAs under review.

Exogenous RP – a reference point given external to the game being played, expected utility of a COA is evaluated relative to that RP

Endogenous RP – a reference point created by interactions of player expected utility in a game

Nash Equilibrium (NE) - Theoretical equilibrium solution to a non-cooperative game. A pure NE means that in theory each player should prefer their equilibrium COA with 100% intent. If all players chose their respective pure equilibrium COAs during one round of the game, the NE solutions mean each player gets their best possible expected utility given all other players are simultaneously trying to maximize their own expected utility. Alternatively, a mixed strategy NE reflects what one player should do over multiple iterations of the game (not factoring in learning) to make their opponent indifferent amongst their own COAs, subject to a probability distribution.

Pathway expected utility (UeT) - the attacker value expected from selecting a specific pathway COA

Course of Action (COA) - here a specific pathway of foreign ports and domestic ports to exploit in moving a weapon of mass destruction into the US, or a specific defender investment decision

FP – Foreign Port

DP – Domestic (U.S.) Port

Notes


Risk, Deterrence, and Prospect Theory: Decision Bias Influence on Quantifiable Deterrence Efficacy in Reducing Risk | By Eric Taquechel


13. This is unclear. The piecewise value function is a function of a specified reference point as presented, although has no ramifications for our approach.


20. One might ask why we do not apply the value function to the UeT itself. Doing so would invert preferences from what CPT would predict.

21. We note that CPT predicts the sum of probability decision weights will be one when all prospects are gains, or when all prospects as losses; however, the sum may not be 1 for a prospect consisting of both losses and gains (Tversky and Kahneman 1992). That said, we do not apply probability-weighting functions in this work, so we keep the original requirements that intent ratios must sum to one.

23. This comports with basic principles of CPT- nonlinear preferences. In our examples presented, expected utility does not necessarily increase linearly, so we calibrated based on linear increase first to confirm our approach for intent ratio calculation under CPT assumptions incorporated some element of nonlinearity.


---

**Copyright**

Copyright © 2022 by the author(s). Homeland Security Affairs is an academic journal available free of charge to individuals and institutions. Because the purpose of this publication is the widest possible dissemination of knowledge, copies of this journal and the articles contained herein may be printed or downloaded and redistributed for personal, research or educational purposes free of charge and without permission. Any commercial use of Homeland Security Affairs or the articles published herein is expressly prohibited without the written consent of the copyright holder. The copyright of all articles published in Homeland Security Affairs rests with the author(s) of the article. Homeland Security Affairs is the online journal of the Naval Postgraduate School Center for Homeland Defense and Security (CHDS).