Working Paper

# Toward Theory for Dissuasion (or Deterrence) by Denial:
## Using Simple Cognitive Models of the Adversary to Inform Strategy

Paul K. Davis

RAND NSRD

WR-1027
January 2014



# Preface

This Working Paper grew out a conference paper presented at the Munk School of the University of Toronto, October 18-20, 2013. The conference, *Deterrence by Denial: Theory, Practice, and Empiricism,* was co-organized by the Munk School of Global Affairs and the Center for Security Studies, ETH Zurich. It included a number of international scholars from a broad range of university and research institutions. As it turned out, there was a good deal new and interesting in the subject, and much fodder for discussion. This Working Paper extends my conference paper and is intended to invite informal peer review before I complete it at a later date. A chapter-length adaptation of that final paper will appear in a book being edited by Andreas Wenger and Alex Wilner.

This research was conducted within the International Security and Defense Policy Center of the RAND National Security Research Division (NSRD). NSRD conducts research and analysis on defense and national security topics for the U.S. and allied defense, foreign policy, homeland security, and intelligence communities and foundations and other non-governmental organizations that support defense and national security analysis.

For more information on the International Security and Defense Policy Center, see http://www.rand.org/nsrd/ndri/centers.

# Table of Contents

# Introduction

## *Purpose*

This chapter has two parts. First, I discuss theory for "dissuasion by denial" by focusing on the adversary's potential reasoning. This redefines and relabels what has been called "deterrence by denial" over the years. I then introduce a simple cognitive model of the adversary, who at best will enjoy limited rationality and may in some respects be non-rational. After applying the model to examples illustrating subtleties, I turn to asking how we might evaluate whether a given defense system (i.e., a system to "deny" success of an attack) is worthwhile. I use a variant of the same model to evaluate illustrative defense options from a friendly perspective, recognizing their potential effects on the adversary, but recognizing also that such options have negative side effects as well as costs. Thus, whether defense options are worthwhile depends on particulars.

The paper is theoretical rather than empirical, but uses examples from conventional defense, ballistic-missile defense, counterterrorism, homeland security, and balance-of-power issues for concreteness.

## *Definitions and Relabelings*

At first glance, the original deterrence by denial concept seems straightforward. More than a half-century ago Glenn Snyder defined it (Snyder, 1960) as deterrence achieved by

> *the capability to deny the other party any gains from the move which is to be deterred* [original]

Snyder was drawing a distinction between this and normal deterrence, which threatens punishment if the action is taken. Snyder's point was important, but the original definition is too stark for my purposes here. Further, it introduced an unfortunate labeling. My view is that extending the definition of deterrence beyond its threat-of-punishment meaning obfuscates distinctions on on which critical reasoning and effective communication depend. In my view, it is far better to refer to the broad concept of *influence theory*, which includes reassurance, co-optation, persuasion, dissuasion,[1] and punishment for recent actions so as to deter future actions,

[1] My ideas on *influence theory* date back to my earlier work on counterterrorism (Davis and Jenkins, 2002). As I learned when presenting that work, Alexander George had introduced the term influence theory many years earlier (George and Smoke, 1974). As he discussed in a later article (George, 2003), influence theory should include consideration of both carrots and sticks, and of reassurances, as discussed by Janice Gross Stein (Stein, 1991). In my earlier work I did not explicitly mention reassurance as part of the influence kit-bag, but do so here.

and to then treat denial as a form of dissuasion.[2] With this relabeling,[3] I suggest the following definition, which is important in what follows:

> *Dissuasion by denial (DND) is deterring an action by having the adversary see a credible capability to prevent him from achieving potential gains adequate to motivate the action.*

This definition refers to what the adversary "sees," whether he regards that as "credible," and whether he sees the "potential" gains as good enough by some criteria. Not just "any" gain is sufficient. The word "potential" avoids assuming that the adversary bases his judgment on expected subjective utility as in rational-actor theory.

## *Discussion*

Given the revised definition, a reasonable question is what the difference is between DND and defense. Arguably, if defense were perfect, affordable, and without negative consequences, focusing narrowly on defense itself would suffice. We wouldn't need to be troubled by such pesky issues as adversary intentions, perceptions, decision style, and other idiosyncrasies. Unfortunately, real defenses—however valuable—are typically imperfect, costly, and troublesome in one way or another.

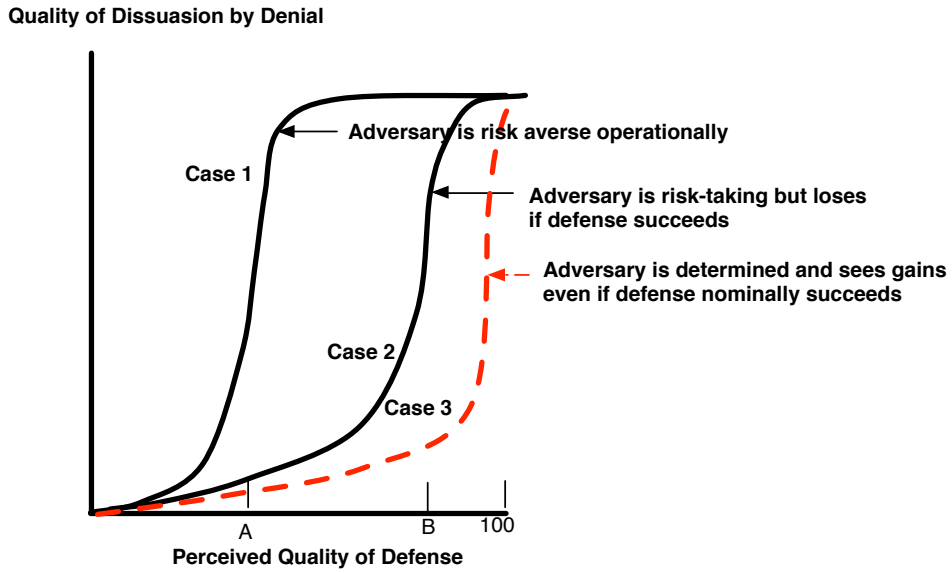
Figure 1 suggests how to think about DND as a function of how good the defense is perceived to be. It asserts that DND may be very effective for a "normal" adversary that is operationally risk-averse if the quality of defense is perceived by the adversary to be sufficiently good—not perfect, but sufficiently good (Case 1). A more determined and risk-taking adversary (who might be ideologically extreme) would be dissuaded only if defense were perceived to be quite good (Case 2). Even more extreme adversaries, however, might see possible strategic gains even if the defense largely succeeds in narrow terms (Case 3).

---

[2] The classic meaning of "dissuade" is to convince someone against an action by advice, exhortation, or persuasion (e.g., Merriam-Webster.com). It has its root in the Latin word "dissuadere" (www.oxforddictionaries.com). In everyday English, "deter" and "dissuade" may be synonyms, but the distinctions are important in more rigorous discussion, as noted recently by John Sawyer (Sawyer, forthcoming). I am aware that the Department of Defense uses "dissuade" to mean something more specialized, as in efforts to dissuade another state not to develop nuclear weapons, a usage that was probably introduced in the Quadrennial Defense Review of 2000-2001 (Rumsfeld, 2001).

[3] In recognition that some readers will wish to cling to the more traditional reference to "deterrence by denial," I use the abbreviation DND throughout the paper.

**Figure 1 Actual and Perceived Quality of Defense**




In support of the ideas in Figure 1, consider that locking automobile doors deters casual car thieves and inebriated teenagers. Drug smugglers can be deterred by counter-narcotics operations that create a small likelihood of capture (say 10-20%) *and* a high likelihood of serious subsequent punishment (Anthony, 2008; Anthony, 2004; Stein and Levi, forthcoming). Conventional military aggression can sometimes be deterred by defenses that merely prevent quick and easy victory (Mearsheimer, 1983). Many committed terrorists can be "operationally deterred" by worries about security forces and the ability to accomplish the particular operation (Morral and Jackson, 2009): they want their operations to be successful (Davis and Jenkins, 2002).

These examples raise the problem that a particular act may be deterred, but the adversary may look elsewhere for an open door, different smuggling strategy, surprise attack, or undefended border. Thus, "denial" must be more comprehensive than blocking one avenue of attack, although looking elsewhere for an "open door" may be a considerable and discouraging obstacle if it means working in unfamiliar territory and unfamiliar ways (Stein and Levi, forthcoming).

With this caveat, much can be done with the construct of Figure 1 so long as we focus on how the *adversary* may perceive "Quality of Defense." The possibilities here are sobering. The adversary may:

1. Underestimate the defense if its more effective elements are difficult for him to see, especially if elements that he does see are weak.
2. Have enough resources to try numerous times. A defense that is quite effective for a single attack may be assuredly vulnerable to multiple attacks.
3. Achieve essential objectives even if the defense is relatively effective. For a rogue state trying to deter intervention by the United States and allies, the rogue's ability to deliver even a single nuclear weapon against an allied capital or U.S. homeland might have great value even if defenses could intercept *most* weapons.[4]
4. Benefit even if attack "fails." Perhaps the fact of the attack will motivate the terrorist organization's followers by showing that it still exists and is showing audacity. Perhaps headlines and public consternation would constitute success.

The conclusions here are that denial capability need not be perfect, but must be assessed in terms from the adversary's perspective, that DND efforts must consider both single and repeated attacks, and that—in some cases—DND will not succeed because benefits accrue to the adversary by visibly attempting the attack, even if it fails.

### *Dissuasion By Denial (DND) Does Not Stand Alone*

It follows from this discussion that DND does not stand well alone. This point bears emphasis because DND is often discussed as though it is a concept apart: we will *either* depend on defense by denial *or* do something else, and if we depend on it, it will or will not work.

Even if we set aside the case of an adversary who sees value in a failed attack, there are other reasons for the conclusion. In particular, even if our defense were extremely good, we would be rightfully nervous as attempted attacks continued. We are pleased when a new al-Qaeda attack is foiled, but are concerned that al-Qaeda is still able to mount attacks and is using new tactics. It is not terribly reassuring that so many attacks have failed over the last decade because good luck has played too big a role.

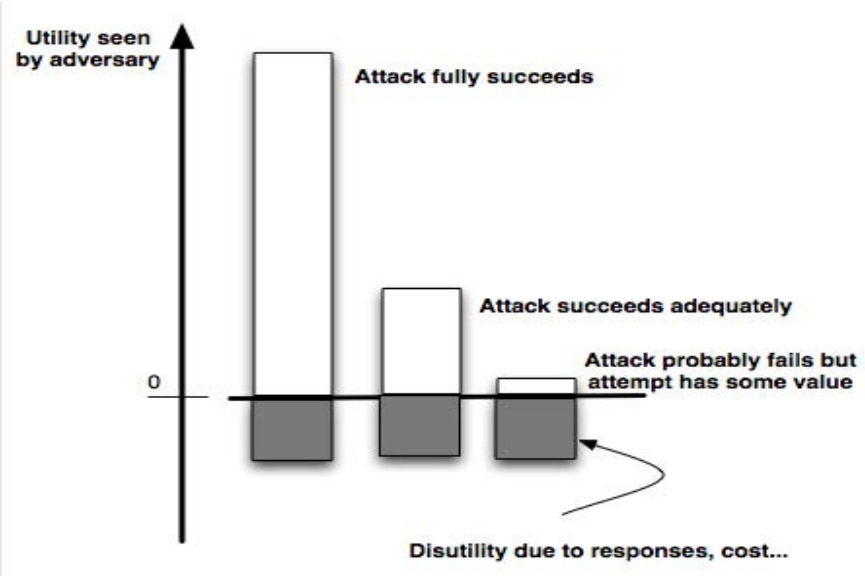
An important element of strategy, then, is to raise the price of attacks. Although the point is elementary, Figure 2 elaborates for explicitness. Assume that the adversary must pay a price of some sort for an attack (the disutility shown with gray shading). For the case of the left-most bar, the attack is successful and well worth the price. It may be worth the price even if the attack is only partially successful (middle bar). What matters for deterrence is that the price paid is greater than the gains that may be achieved (rightmost bar). To summarize:

---

[4] This point has not been lost on allies to whom the United States seeks to extend deterrence (Harvey, forthcoming).

- Dissuasion by Denial (DND) does not stand alone. The larger strategy should include elements of deterrence by threat of punishment, other mechanisms for imposing costs (even opportunity costs), and other types of influence as described later. This is especially true if the adversary has the resources for repeated attempts.[5]

**Figure 2 Deterrence Depends on Both Positive and Negative Benefits**




## *Effects of Uncertainty.*

So far, I have reasoned implicitly in the terms of expected values, as in the tradition of usual decision analysis. What happens if we consider uncertainty? The adversary will often be quite uncertain both about the likelihood of proximate success (e.g., penetration of defenses) and the resulting outcome. For example, if the attacker hopes for a sudden collapse of will and morale (as with a rapid decisive operation in conventional warfare),[6] or to create widespread chaos and paralysis after a strike on a city (whether of 9/11 magnitude or something larger, even to include chemical, biological, or nuclear weapons), then the hoped-for utility would be based on far more than direct damage.

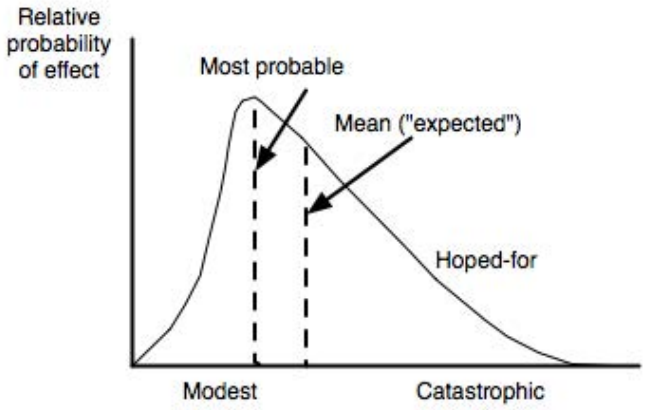
---

[5] This is recognized to some extent by U.S. operations planners who have "stretched" the meaning of deterrence to include, e.g., encouraging adversary restraint by offering or pointing out benefits of such restraint (USSTRATCOM, 2010, p.27). As mentioned earlier, I believe that it would be better if the corresponding doctrine were expressed in terms of "influence theory," which would clarify the issues and broaden the space for strategy development.

[6] This refers to a concept of operations suggested in the late 1990s (Ullman and Wade, 1996), one inspired by, e.g., the quick and easy successes of Nazi Blitzkrieg operations. Such operations are sometimes quite feasible, but depend on many favorable circumstances as discussed in (Echevarria II, 2001).

Figure 3 illustrates how an optimistic and perhaps grandiose adversary might think about the potential consequences of an attack. With this assessment, even a rational-analytic calculation would put a much higher value on attacking than suggested by the most-probable outcome (or even the "expected value"). Yes, the attack might fail; yes, it might only accomplish something relatively modest; but *perhaps* the effect would be catastrophic (note the long "tail" to the right). Regrettably, one of the lessons learned by terrorists after 9/11 was that effects can indeed be far greater than expected, as acknowledged by Osama bin Laden in a taped discussion (Washington Post, 2001). Although al Qaeda hoping to evict Western influences and reestablish the Caliphate qualifies as grandiose in our thinking, it is part of al Qaeda's lore that the Mujahideen defeated the Soviets (see, e.g., 2005 interview with al Zawahari in a reader ((Ibrahim, 2007)).

**Figure 3 The Expected Subjective Mean Is Not the Whole Story**




Note: the chart is merely schematic.

## *Uncertainty about Non-Rational Considerations*

So far, I have assumed at least limited rationality. Determined and creative authors have sometimes found it possible to discern rationality even with behaviors that would usually be regarded as utterly irrational. Doing so is sometimes appropriate, as when analysts work harder to appreciate the objectives, value functions, and perceptions of the target of influence—far better, certainly, than mirror-imaging. Altruism, for example, can motivate people to do what would be irrational in a narrow construction of objectives and values (Berrebi, 2009). Sometimes, however, the effort to stretch versions of the rational-actor model are manifestations of a strongly-felt desire to salvage the theory, even when it's a bad theory. Although some argue to the contrary that it is just a matter of having the right utility functions, their argument collapses if the utility function inferred from behavior is unstable—reflecting the immediate and particular circumstances. Stable utilities are an essential condition for utility theory to have substantive content or to be falsifiable. With this in mind, consider the following individual- and

group-level examples:

1. The behavior of someone (even a head of state) who is frightened, desperate, humiliated, and willing to try anything to get out of a situation. The tendency may be to "do something," even if the objective odds of success are low. Alternatively,the result could be abject paralysis.
2. The behavior of someone who is enraged and keen on generalized revenge against the "others" who have attacked him
3. The behavior of disciplined soldiers instructed to charge into machine-gun fire in which they feel certain they will die
4. The behavior of religious zealots willing to martyr themselves even thought their attack is certain to fail
5. The uncertain behavior of religious zealots with apocalyptic views
6. The behavior of a mob, which can settle or instead explode into a riot with undetermined objectives

Some encouraging considerations are that people who may not be deterrable or dissuadable at one time may become so later. Even zealous religious warriors, for example, may lose their ardor for martyrdom (Bjorgo and Horgan, 2009; Horgan, 2009). Even highly disciplined soldiers will sometime disobey the orders of an officer whom they see as having lost his mind or legitimacy. People who are enraged, humiliated, desperate, and/or frightened may have somewhat different emotions in the morrow, or when circumstances change. People willing to give their lives in a cause may decide against giving their lives if doing so would not accomplish anything worldly.

My reasons for this brief section is simply to note that deterrence and dissuasion are not always going to be effective. With this background pointing out some of the subtleties of DND, let me next turn to how we might assess DND with simple cognitive models. The initial discussion assumes considerable rationality; subsequent discussion includes nonrational factors.

## A Simple Model for Cases of Limited Rationality

### *The Model's Structure and Features.*

There is little reason to examine a fully rational actor because such entities probably exist only in text books or very special circumstances. Suppose, however, that the adversary at least attempts to make an intelligent decision after having considered the pros and cons of alternatives. I refer to this as the adversary having *limited rationality*: "limited" because the results may be

flawed for reasons discussed below.

Table 1 describes the framework of a simple cognitive model for an adversary with limited rationality. It focuses on the *adversary's* mental frame. For simplicity of example, it depicts the adversary as having three options in a particular instance: do nothing different (the baseline), take the action X that we're trying to deter, or do something else. Framing the decision as one of choices among options is part of what makes this a cognitive model of limited rationality rather than a behavioral model. Even if the adversary recognizes that prospects are poor if he takes Action X, taking the action might be attractive relative to alternatives. Conversely, the action might have some attraction, but less than that of some other action. Noting the columns for worst-case and best-case outcomes, we see that this framing is not that of usual "decision theory,"[7] where the actor would pick the option with the highest expected subjective utility (Fischoff, Goitein, and Shapira, 1981). Despite the long and distinguished literature on the normative virtues of maximizing expected subjective utility going back to Frank Ramsay, John von Neuman, Leonard Savage, and others, it has been recognized for decades that real people often do not reason in this way. The long-standing focus on the rational-actor model is puzzling.[8] Finally, note that Table 1 allows for alternative models of the adversary, here called Model A and Model B.[9]

---

[7] It is unfortunate that the general terms "decision theory" and "decision analysis" were appropriated decades ago by those with a particular view of how decisions are or should be made.

[8] A few authors in political science have noted this over the years (Jervis, 1976; Jervis, Lebow, and Stein, 1985). Patrick Morgan has also noted perceptively that deterrence theory need not have been based on the rational-actor model (Morgan, 1983; Morgan, 2003, pp. 42-78). Many psychologists since the early work of Daniel Kahneman and Amos Tversky have expressed puzzlement about why the insights have been taken up so slowly (Slovic, Fischoff, and Lichtenstein, 1977).

[9] My work on cognitive modeling began with computer modeling during the Cold War (Davis, 1989a) and continued in more reductionist fashion with John Arquilla as we studied Saddam Hussein in 1990-1991 (Davis and Arquilla, 1991b; Davis and Arquilla, 1991a). Ideas were also summarized elsewhere (Naval Studies Board and National Research Council, 1996; Kulick and Davis, 2003). Saddam Hussein's actual thinking in 1990-1991 and 2003 is now much better understood because of extensive interviews and documenatary information (Woods, 2008). The 1991studies got many things right, but there also were surprises. A theme of the Davis-Arquilla work was the need to use *alternative* adversary models (even two is much better than one) so as to encourage hedging in strategy—hedging against both more optimistic and more pessimistic possibilities. It is not prudent to assume that we can build a "correct" cognitive model of an adversary.

**Table 1 A Simple Cognitive Model**

| | Subjectively and qualitatively estimated with deep uncertainty | | | | |
|---|---|---|---|---|---|
| Option | Worst-case outcome | Expected outcome | Best-case outcome | Net Assessment | |
| | | | | Model A | Model B |
| Do nothing different | | | | | |
| Conduct Attack X | | | | | |
| Do something else | | | | | |

Note: Net Assessment is a function of the preceding columns, but also depends on the decision maker (e.g., Model A or B)—e.g., on the decision maker's risk-taking propensity or passion for the possibility of a best-case outcome.

This conceptually simple model can be remarkably rich if we take care in estimating the cell values by taking into account, as best we can, considerations of the adversary's information; heuristics, biases, and intuitive thinking; values; and personality.

*Information.* As observed by Herbert Simon starting in the 1950s (Simon, 1978), people frequently lack the information necessary for the decision-analytic calculations, cannot realistically obtain it, and—even if they had it—would find the calculations impossibly difficult because of uncertainties and time constraints. Thus, Simon argued, people use heuristics—short-cut methods for making decisions that are good enough and situation dependent. He referred to this as bounded rationality. An implication is that, in Table 1, the cell values should refer to the adversary's perceived information and reflect his shortcuts.

*Heuristics, Biases*, *and Intuitive Thinking.* Bounded rationality is only part of the story. As richly documented by Daniel Kahneman, Amos Tversky, and subsequent researchers, people routinely act in ways that standard rational-actor model regards as erroneous or at least as suboptimal—even when they have the information and, in principle, can make the calculations (Kahneman, 2002). Real-world decisions are often said to be "afflicted" by cognitive biases or, at least, to often be driven by the "fast thinking" mode of our brains (Kahneman, 2011). That said, intuitive or naturalistic decisions are sometimes fast, inexpensive, efficient and even superior to those from an allegedly rational-analytic process (Klein, 1998; Gigerenzer and Selten, 2002). Good leaders, for example, sometimes make wise decisions by "knowing" that what matters most is outside the framework posed by decision analysts or that actual risks are greater than those accounted for in the decision analysts. In our day-to-day lives, a wise person may value some subtle personal relations more than the economic benefits being addressed. At a more cosmic level, U.S. and Soviet leaders during the Cold War knew viscerally that—independent of calculations about who would "win" a nuclear counter-force exchange, or who had the upper hand in terms of weapon-systems power, nuclear war would be a catastrophe and they should

assure that it did not occur.[10]

A good modern-day understanding of human decisionmaking is one that recognizes that it is not just that humans don't always follow the rational-analytic model (i.e., that description and prescription vary). Rather, humans benefit from having a combination of fast and slow, i.e., naturalistic/intuitive and rational-analytic, styes of reasoning. Which is better depends on circumstances and hybrids are often desirable.[11]

*Values.* A third shortcoming of the usual rational-analytic discussion of decisionmaking is that the calculable expected value of utility is not necessarily what people want to maximize. Consider a "great conqueror" as he contemplates whether to start a next campaign. He may be uninterested in the expected value of outcome, since he will only live once. He may instead wish to maximize the probability of achieving a historically unprecedented empire. Think about Napoleon's march into Russia, despite being aware of risks. This type of behavior might be expected by especially narcissistic personalities. As mentioned earlier, values are situational in that how people evaluate options depends on history, cues, and emotional considerations, including the celebrated effect of Kahneman-Tversky prospect theory (sometimes called loss-aversion theory) by which people—in some circumstances—value not losing something more than they valued gaining it.

*Personality*. Ultimately, in attempts to deter, dissuade, or otherwise influence, the target of our efforts are living individuals or groups, which implies that we should seek to understand their character and personality, which relates to their values, intuition, perceptions, heuristics, and biases. Ironically, many analysts hesitate to attempt this, perhaps because they believe it is too hard or because they believe that "structural considerations" such as power balances will dictate behavior. That the effort is difficult is surely true in many cases, but I am among those who think it obvious that the character and "personalities" of leaders and leadership groups matter, sometimes greatly, as was the case in the Cuban Missile Crisis. I am in good company.[12]

---

[10] Although the rational-analytic approach can be wiser than this suggests, it is striking that throughout the Cold War, too many analysts—including scholars—obsessed on the so-called "calculus of deterrence" focused on measures such as the post-exchange ratio of counter-force power. Such analysis was a major source of dangerous ideas that could have been quite destabilizing in crisis (Davis, 1989b).

[11] See a monograph and a subsequent paper suggesting how staffs can support both rational-analytic and intuitively oriented decisionmakers (Davis, Kulick, and Egner, 2005; Davis and Kahan, 2006). These did not have the benefit of Kahneman's recent book (Kahneman, 2011), which reframes issues into the pros and cons of the fast and slow modes of decisionmaking, and credits the work and ideas of the naturalistic school. A decade earlier, the battle between schools had sometimes appeared epic and even bitter.

[12] The significance of the *person* making decisions is discussed in two books (Post, 2008; Schneider and Post, 2004), the latter with chapters on suicide bombers, Kim Jong-Il, Saddam Hussein, and Muammar Qaddafi and a highly

### *Using the Model: Diagnosis*

The model of Table 1 cannot deal with all of the complications and subtleties, but at least it recognizes that decisions may be affected by worst- or best-case considerations, not just the "expected" value. Further, it recognizes that different decision makers will reach different net assessments in the same circumstances, depending on, e.g., how risk-taking they are and how passionate they are about "going for the gold" (the best-case outcome). The need to recognize such person-dependent considerations appears to me fundamental to understanding deterrence and dissuasion.

Finally, as shown below, Table 1 allows us to see how misperceptions and miscalculation can lead to what might otherwise appear to be bizarre conclusions. The most important examples are different depending on whether the adversary is effectively being aggressive or defensive.

Aggressive Adversary

1. Imagines an extremely favorable outcome to be far more likely than it actually is
2. Fails to recognize how bad the worst-case outcome could be or how likely the outcome is—perhaps ignoring risks below a threshold of perceived likelihood even if the consequences would be catastrophic if the outcome occurred[13]
3. Even with accurate understanding of upside potential and downside risk, dwells cognitively on the upside

Defensive Adversary

1. Perceives the consequences of continuing current strategy as most likely to be disastrous (e.g., as Japan saw the situation in 1941 as the United States and Great Britain were thwarting its imperial ambitions)
2. Perceives Attack X as the "only chance" for survival or for averting calamity
3. Does not recognize or take seriously options that would mitigate problems with the status quo without involving conflict

---

relevant paper by Alexander George (George, 2003).

[13] This thresholding phenomenon is evident from personal-life experiences and is also remarked upon in the empirical literature, such as that puzzling about why people are more likely to buy insurance for relatively probable but moderate-consequence risks than to buy reasonably priced insurance for unlikely but catastrophic possibilities (Camerer and Kunreuther, 1989). As with many of the heuristics, they may seem irrational, but are actually quite valuable as rules of thumb. Without this thresholding, we might find it difficult to get out of bed in the morning to face the world that is so full of risks.

The terms "aggressive" and "defensive" are arguable here because an aggressor will often rationalize his action as being defensive, and someone being defensive may take actions seen as aggressive. The reader will probably agree, however, with the contrast between being driven by the potential for gaining power at one extreme or by the imminent mortal danger at the other extreme. Still, categorizing is tricky. North Korea and Iran, for example, have had good reason to be fearful.[14] In contrast, no one could claim that Hitler was being fearful in his invasions. The story is more complex with al Qaeda. To Ayman al-Zawahiri, the Muslim world has long been under attack by the West—first by the effective and insidious method of "Masked Agents" (e.g., Hosni Mubarek and the Saudi Royal Family doing the West's will) and later by invasion of Afghanistan and Iraq.[15] Al-Qaeda's attacks have been part of a strategic-level effort to deter and compel the West. As noted a decade ago, al-Qaeda's top leaders are not very susceptible to deterrence by threat of punishment, but "al-Qaeda" should be seen as a system with many components and entities (Davis and Jenkins, 2002), many of which are subject to various influences, including deterrence and dissuasion, including events that create political opportunities for people who have lived under tyranny or which discredit the moral legitimacy of the al-Qaeda organization.[16] The model illustrated by Table 1 can be broadly useful by applying it separately to different individuals or groups within an al-Qaeda or even an adversary nation.

### *Using the Model: Prescription.*

Let us now apply the simple cognitive model notionally but consider influences that can be brought to bear as suggested byred dashed lines in Figure 4. If we are attempting to deter Action X, then we should want the adversary to see better alternatives, to have greater fear of worst-case consequences of Action X, to expect less from Action X, and to put aside notions of the great and glorious best-case outcome. Further, as discussed earlier, we would want him to see costs. They might be from a retaliatory attack, blow-back from his own supporters (e.g., from allied countries or his own population), or direct costs. Perhaps an attack would deplete his resources (e.g., if he had only a few weapons, rockets, or competent human teams). Perhaps it would be expensive for him to make the attack and his resources are limited. Again, then, DND alone is not a good strategy.[17]

---

[14] Presumably, they paid attention to the Axis of Evil discussion in the 2002 State of the Union address by President George W. Bush and the book by his ex speech writer and another prominent political figure (Frum and Perle, 2004).

[15] For the al-Qaeda narrative, see a book (al-Zawahiri, 2001) and various parts of a "reader" (Ibrahim, 2007).

[16] A review discusses motivation for terrorists and their supporters (Davis and Cragin, 2009).

[17] This approach was used in an unpublished paper with Anastasia Norton on strategic communications in a summer study of the 2010 Summer Hard Problem (SHARP) of the Office of the Director for National Intelligence and my

**Figure 4 Influences on the Factors of the Simple Cognitive Model**

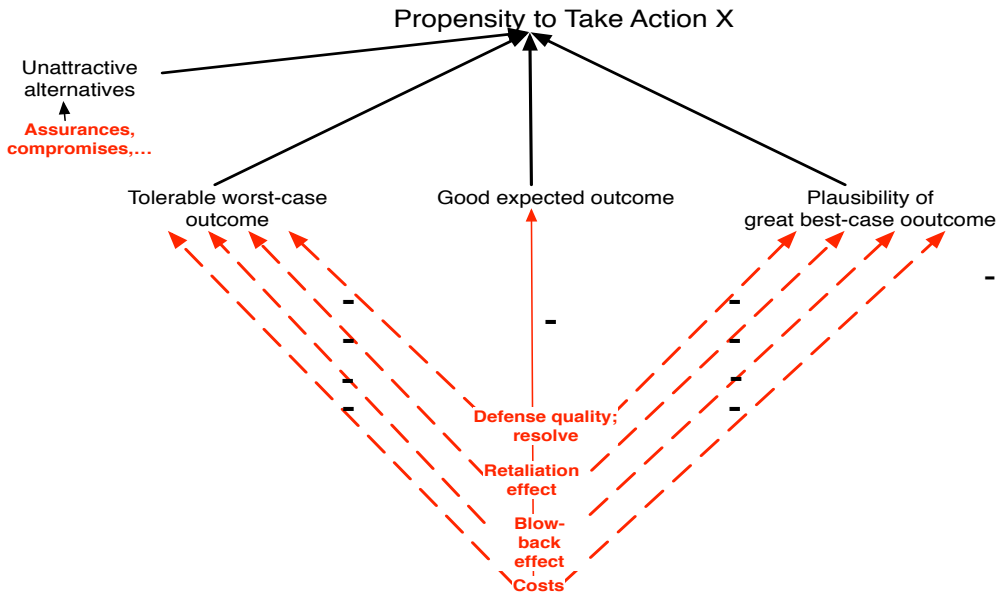



Figure 4 reminds us of how various influences interact, but says nothing about how the factors affecting decision combine—i.e., about the functional dependence of Propensity to Take Action X on the four contributing factors. Tolerable worst-case outcome, etc.? Details are hard to estimate, but some mechanisms for affecting the calculation in desirable ways may include the following. The first two seek to affect how calculations are made; the latter two seek to affect the perceptions as the adversary evaluates the worst, expected, and best outcomes for each option. All relate, arguably, to helping the adversary overcome cognitive biases.

1. Dramatize—in diplomacy, public statements, and actions the potential for disastrous worst-case outcome (e.g., nuclear war, regime change and hanging), thereby increasing the salience (and psychological availability) of the worst-case and perhaps reducing risk-taking propensity.
2. Dissuade or persuade by elevating the plausibility of good outcomes under other options than Action X—i.e., make them plausible enough so that they are actually considered by the adversary rather than ruled out heuristically.
3. Undercut the plausibility of the best-case outcome (e.g., demonstrate resolve, prepare for long war, or maintain imperfect defenses adequate to preclude quick and easy victory).[18]

---

contributions to a DoD Strategic Multi-Layer Assessment of violent extremism (Davis, 2012).

[18] The value of this was highlighted in a influential book about the conventional military balance (Mearsheimer,

4. Make expected outcome more costly by increasing the likelihood of effective retaliation, international sanctions, and so on. That is, reintroduce the deterrence-by-punishment mechanism.

For the most part, these items merely express the obvious. However, matters become less obvious when we recognize tensions related to the security dilemma famously described by Robert Jervis (Jervis, 1976). For example, efforts to demonstrate resolve and prepare for extended war (thereby precluding the adversary's quick and easy victory) may be indistinguishable to the adversary from preparing for war. Efforts to raise costs, such as organizing international sanctions may also be seen (and may in fact be) threatening. Unfortunately, assurances or diplomacy with the prospect of compromise might calm the adversary but create problems in domestic politics, as illustrated by the efforts of U.S. Senators in late 2013 to add further sanctions against Iran, despite protestations by the Obama administration that such sanctions, even if provisional, would only poison the well of fragile diplomacy on nuclear matters (Warrick and DeYoung, 2013).

## Is the Defense Worth the Candle?

So far, I have discussed the role of defense in deterrence. A different question is whether how to assess the value of defenses given that they are imperfect and come with substantial economic and social costs. How much is enough? And of what kind of defense? The issue has become particularly important in recent times in at least three domains:

1. Conventional military actions taken to improve general deterrence against regional aggression by China (e.g., the "tilt" to Asia and the Air-Sea Battle)
2. Homeland ballistic-missile defenses against attacks by rogue states such as North Korea or Iran
3. Homeland-security defense measures for detecting possible terrorists (particularly use of behavioral indicators of violent malintent and monitoring of cyberspace, of which I discuss only the former).

---

1983). At the next level of detail, analysis demonstrated that precluding a short-mobilization attack would go far in precluding a quick-and-easy Soviet victory and that conventional arms control should focus on that objective rather than across-the-board force reductions (Davis, 1988). This was promoting a version of DND focused on raising risks and preventing quick-and-easy victory.

## *A Framework for Considering Options.*

Table 2 is a relatively simple framework for considering defensive options, with some features in common with the simple cognitive model presented earlier for deterrence. The primary points are that a defensive approach should be evaluated for both its effectiveness in defending against potential attack, and also for its positive and negative side effects. The positive side effects might include providing some degree of assurance to the citizens being defended (assurance that may be a function of the actual effectiveness), the fact that the government is seen as "doing something," or both. The negative side effects can include raising the level of threat perceived by the adversary (the security dilemma), interfering with commerce, and intruding on the privacy and other civil liberties of citizens. As with Table 1, but thinking now in terms of our own reasoning, the model in Table 2 provides for alternative models (Models X and Y), to recognize that within our own society, people will combine the various considerations differently. Here the models are better seen as representing different "perspectives." Illustrating the effects of even two contrasting perspectives tends to encourage more open-minded discussion and, sometimes, hedging strategies as discussed in work on strategic portfolio analysis (Davis, Shaver, and Beck, 2008; Davis, 2014)

**Table 2 A Simple Model for Thinking about Defense Options**

| Option | Minimum effectiveness | Mean effectiveness | Maximum effectiveness | Net effectiveness | Positive side effects | Negative side effects (e..g., civil liberties) | Cost | Overall assessment | |
|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | Model X | Model Y |
| 1 | | | | | | | | | |
| 2 | | | | | | | | | |
| 3. | | | | | | | | | |

## *Some Examples.*

*Air-Sea Battle*

As a first example, consider the defense strategy being taken in attempting to improve the quality of deterrence in Asia. One aspect, the Air-Sea Battle (Department of Defense, 2013), is particularly controversial. As so often happens in thinking about deterrence—the *effectiveness* of the approach is easy to debate but difficult to assess. The United States and China have enormous incentives to avoid crisis and conflict, in which case relatively modest measures such as Air-Sea Battle might have substantial deterrent effects. Unfortunately, it is possible that there will be

negative effects from security-dilemma dynamics. The Air-Sea Battle concepts have elements of deterrence by threat of punishment and dissuasion by denial, but also have escalatory elements that could be destabilizing (Gompert, 2013). The United States is clearly feeling its way as strategy for the Asia Pacific region evolves.

*Ballistic-Missile Defense*

As a second example, consider deployment of ballistic missile defenses as begun in the George W. Bush administration with emplacements in Alaska and Vandenberg Air Force Base in California. Public discussions on the matter vary, but Directors of the Missile Defense Agency have expressed confidence that the system is working to defend the United States (U.S. Senate Armed Services Committee, 2013), if not as well as it will over time. In ordering its deployment in the early 2000s, Secretary of Defense Donald Rumsfeld made it clear that he believed improvements would occur with experience (and only with experience rather than just prolonged R&D). Although he may not have used this phrase, my interpretation from various report and statements (Rumsfeld, 1998) has been that the baseline option of *not* deploying defenses, and of remaining "naked to attack" by a rogue state such as North Korea was simply unacceptable to Rumsfeld and President Bush. Even some effectiveness was a great deal better than none, and effectiveness would improve. Part of the argument is that the deterrence probably increase quickly with deployment (see Figure 1), even if effectiveness is limited. The counterargument by critics is that the system being deployed can be readily defeated by countermeasures that could be mounted by any nation-state able to develop and field ICBMs (Sessler et al., 2000). A counter-counter argument is that the adversary does not know precisely how the U.S. BMD system works or what counter-counter measures it employs. Such arguments can only be assessed well within the classified world. However, they are increasingly important to the U.S. and the allies to which the United States wants to credibly extend not just deterrence of attack by weapons of mass destruction, but deterrence from conventional aggression. In any case, homeland BMD effectiveness remains questionable and hardly something to be taken for granted just because we have operational forces (National Research Council, 2013; Coyle, 2013).

As for positive and negative side effects to defenses, there may be a positive, reassuring effect within the U.S. that would strengthen resolve in crisis. On the other hand, some critics argue that deploying a system that has not been substantially tested undercuts the integrity of DoD's acquisition system and may be providing a baseless sense of confidence—a significant side effect. Also, some U.S. BMD developments and deployments have contributed to foreign policy tensions with Russia, even though the system is not oriented toward nor effective against Russia. The most important negative, however, is simply that the system has uncertain effectiveness but high costs in a period of austerity.

*Homeland-Security Measures*

As a last example, let us consider a class of counterterrorism initiatives reviewed recently in a study that I led with colleague Walt Perry that involved observing the behaviors of individuals and groups at airports, train stations, and other security points Davis et al., 2013. These vary considerably, but include watching for indicators that may suggest apprehension or deception, asking routine questions of some people in line, or even selecting people for more aggressive interrogation in side rooms. Some observational methods attempt to detect subtle behaviors that are difficult to control, such as micro-expressions. Others attempt to detect warning indicators from voice analysis by either human questioners, machines, or both.

If we follow the structure of Table 2 to evaluate such program(s), the challenge becomes interesting technically and as a matter of policy. The effectiveness of the various individual behavioral measures is difficult to evaluate. If the measure is an increased probability of detecting someone with mal-intent, then some of the measures appear to have promise—no surprise to law-enforcement officials for whom the keen eye of the experienced patrolman has long been a key to spotting suspicious activity. However, none of the measures are reliable and most have very high false-alarm rates. That said, it is possible that combining the information from a number of weak indicators (i.e., through networking and fusion methods) could significantly increase detection rates and reduce false-alarm rates. This is most plausible if prior information identifies individuals that merit more careful scrutiny. With a little imagination, one could contemplate every passenger's life record being available for near-real-time computer evaluation along with the at-the-time behavioral observations and physical data on, e.g., where the individual first began this trip, what path he has taken, what passport he holds, his criminal record, and so on. In the wake of a failure to detect a terrorist (as with the Christmas Bomber, who tried unsuccessfully to detonate an underwear bomb over Detroit), the news media is filled with accusations—some of them justified—about how the security system had not appropriately "connected the dots." If one really wishes to connect all dots, even if sometimes erroneously, then the pressures to move toward what critics call the surveillance state are strong. The risks to privacy and civil liberties are substantial, however, as discussed in a National Academy study led by Charles Vest and William Perry (Perry, Vest, and Committee, 2008) and as discussed in the ongoing furor about the wholesale collection of personal metadata by the National Security Agency (Sanger and Savage, 2013).

Returning now to dissuasion by denial, it seems reasonable to believe that imperfect security systems will have a much greater effect by virtue of dissuasion than would be expected from their detection effectiveness alone. Thus, in the terms of Table 2, the security measures have thigh upside potential but may fail because of inherent limitations and adversary

countermeasures. Still, it would seem that even expensive and imperfect methods would be worthwhile if the methods are "good enough." Unfortunately, the methods have numerous negative side effects. These range from the annoyance of having to stand in line and the somewhat greater annoyance of being asked questions and observed, to the substantial impositions that occur when harmless passengers are subjected to hours of interrogation, miss their flights, and perhaps miss appointments or have their vacations ruined. To make things worse, people may understandably feel that they have been unfairly accused, discriminated against, and humiliated. This a a very serious side effect; it also undercuts public faith in the system and its fairness and makes it less likely that affected people will cooperate with—much less actively provide information to—security officials.

One conclusion from our study, then (Davis et al., 2013), was that the U.S. Government should do far more to establish mechanisms for assessing actual effectiveness of defensive methods. This should include routinized collection of sound empirical data and, importantly, subjecting assessments to rigorous peer review—as open as possible, but within classification boundaries if necessary. A second conclusion was that the government should more seriously than in the past the need to reduce the negative consequences of intrusive measures. The steps that could be taken are familiar in the commercial sector and local law enforcement. These include demonstrating respect for people, taking special measures to expedite their processing after delays, compensating them financially , apologizing sincerely for inconvenience, and thanking them for their cooperation. Another class of steps involves severely punishing officials or operators who abuse their access to information or who fail to treat citizens well, and making it difficult for them to do so in the first place. That is, both deterrence by threat of punishment and dissuasion by denial apply within the security system also. Such steps seem obvious, but are not the norm today.

### *Wrap-Up*

In summary, I have sought to accomplish several purposes in this paper. First, I relabeled and refined the definition of deterrence by denial, calling it dissuasion by denial (DND) and discussing some of its more subtle aspects. Second, I introduced a simple cognitive-model methodology for estimating the potential value of DND efforts, emphasizing the need to view the issue through the perspective of an adversary with limited rationality and possible erelements of non-rational behavior. I then turned to the question of when denial efforts (i.e., defensive measures) are worthwhile. Again, I introduced a simple model structure for evaluating issues. A primary objective was encouraging an approach that includes sound technical analysis, appreciates the value of exploiting uncertainty when attempting deterrence and dissuasion, and recognizes that some defensive measures have substantial negative consequences that should

either lead to discarding the measures or mitigating the negative consequences to the maximum extent possible.

## Bibliography


al-Zawahiri, Ayman (2001), *Knights Under the Prophet's Banner*, London: FBIS-NES-2002-0108.

Anthony, Robert W. (2004), "A Calibrated Model of the Psychology of Deterrence," *Bulletin on Narcotics*, Vol. LVI, pp. 49-64.

——— (2008) "Deterrence: An Empirical Psychological Model," *Wiley Handbook of Science and Technology for Homeland Security*, Wiley, p.

Berrebi, Claude (2009) "The Economics of Terrorism and Counterterrorism: What Matters and Is Rational-Choice Theory Helpful?," in Paul K. Davis, and Kim Cragin, eds., *Social Science for Counterterrorism: Putting the Pieces Together*, Santa Monica, Calif.: RAND Corp., pp. 151-208.

Bjorgo, Tore, and John Horgan (2009), *Leaving Terrorism Behind: Disengagement From Political Violence*, New York: Routledge.

Camerer, Colin F., and Howard Kunreuther (1989), "Decision Processes for Low Probability Events: Policy Implications," *Journal of Policy Analysis and Management*, Vol. 8, No. 4, pp. 563-592.

Coyle, Philip E. (2013), "Back to the Drawing Board: the Need for Sound Science in U.S. Missile Defense," *Arms Control Today*, Vol. January/February, p. online.

Davis, Paul K. (1988), *Toward a Conceptual Framework for Operational Arms Control in Europe's Central Region,* R-3704, Santa Monica, Calif.: RAND Corp. As of August 8, 2013: http://www.rand.org/pubs/reports/R3704.html

——— (1989a), *Some Lessons Learned From Building Red Agents in the RAND Corp. Strategy Assessment System,* N-3003-OSD, Santa Monica, Calif.: RAND Corp.

——— (1989b), *Studying First-strike Stability With Knowledge-based Models of Human Decision Making*, Santa Monica, Calif.: RAND Corp.

——— (2012), *Influencing Violent Extremist Organizations and Their Supporters Without Adverse Side Effects,* WR-909-OSD, working draft, Santa Monica, Calif.: RAND Corp. As of As of April 20, 2013: http://www.rand.org/pubs/working_papers/WR909.html.

——— (2014), *Analysis to Inform Defense Planning Despite Austerity*, Santa Monica, Calif.: RAND Corp.

Davis, Paul K., and John Arquilla (1991a), *Deterring or Coercing Opponents in Crisis: Lessons From the War With Saddam Hussein*, Santa Monica, Calif.: RAND Corp.

——— (1991b), *Thinking About Opponent Behavior in Crisis and Conflict: a Generic Model for Analysis and Group Discussion*, Santa Monica, Calif.: RAND Corp.

Davis, Paul K., and Kim Cragin, eds. (2009), *Social Science for Counterterrorism: Putting the Pieces Together*, Santa Monica, Calif.: RAND Corp.

Davis, Paul K., and Brian Michael Jenkins (2002), *Deterrence and Influence in Counterterrorism: a Component in the War on Al Qaeda*, Santa Monica, Calif.: RAND Corp.

Davis, Paul K., and James P. Kahan (2006), "Theory and Methods for Supporting High-level Decision Making," in *Proceedings of Enabling Technologies for Simulation Science X. Edited by Trevisani, Dawn A.*, pp. paper 6227-14.

Davis, Paul K., Jonathan Kulick, and Michael Egner (2005), *Implications of Modern Decision Science for Military Decision Support Systems*, Santa Monica, Calif.: RAND Corp. As of August 12, 2013: http://www.rand.org/pubs/monographs/MG360.html

Davis, Paul K., Walter S. Perry, Ryan Andrew Brown, Douglas Yeung, Parisa Roshan, and Phoenix Voorhies (2013), *Using Behavioral Indicators to Help Detect Potential Violent Acts*, Santa Moncia, Calif.: RAND Corp. As of August 13, 2013:
http://www.rand.org/pubs/research_reports/RR215.html

Davis, Paul K., Russell D. Shaver, and Justin Beck (2008), *Portfolio-analysis Methods for Assessing Capability Options*, Santa Monica, Calif.: RAND Corp. As of August 11, 2013:
http://www.rand.org/pubs/monographs/MG662.html

Department of Defense (2013), *Air-Sea Battle: Service Collaboration to Address Anti-Access and Area Denial,* Washington, D.C.: Department of Defense.

Echevarria II, Antulio J. (2001), *Rapid Decisive Operations: an Assumptions-Based Critique,* Carlisle Barracks, Penns.: Strategic Studies Institute, U.S. Army War College.

Fischoff, Baruch, Bernard Goitein, and Zurl Shapira (1981), "Subjective Expected Utility: a Model of Decision-Making," *Journal of the American Society for Information Science*, Vol. 32, No. 5, pp. 391-399.

Frum, David, and Richard Perle (2004), *An End to Evil: How to Win the War on Terror*, Ballantine Books.

George, Alexander L. (2003) "The Need for Influence Theory and Actor-Specific Behavioral Models of Adversaries (available on-line in Comparative Strategy, Vol. 22 (5), 2003)," in Barry R. Schneider, and Jerrold M. Post, eds., *Know Thy Enemy: Profiles of Adversary Leaders and Their Strategic Cultures (2nd. ed.)*, Maxwell Air Force Base, Ala.: Air War College, pp. 271-310.

George, Alexander L., and Richard Smoke (1974), *Deterrence in American Foreign Policy*, New York: Columbia University Press.

Gigerenzer, Gerd, and Reinhar Selten (2002), *Bounded Rationality: the Adaptive Toolbox*, Cambridge, Mass.: MIT Press.

Gompert, David C. (2013), *Sea Power and American Interests in the Western Pacific*, Santa Monica, Calif.: RAND Corporation.

Harvey, Frank (forthcoming) "Denial and Ballistiic Missile Defense: Old and New Perspectives," in Andreas Wenger, and Alex Wilner, eds., *Deterrence by Denial: Theory, Practice, and Empiricism*, p.

Horgan, John (2009), *Walking Away From Terrorism (political Violence)*, Routledge.

Ibrahim, Raymond (ed. and translator) (2007), *The Al Qaeda Reader*, New York: Broadway Books.

Jervis, Robert (1976), *Perception and Miscperception in International Politics*, Princeton, NJ: Princeton University Press.

Jervis, Robert, Richard.N. Lebow, and Janet G. Stein (1985), *Psychology and Deterrence*, Baltimore: Johns Hopkins University Press.

Kahneman, Daniel (2002), *Maps of Bounded Rationality: a Perspective on Intuitive Judgment and Choice (nobel Prize Lecture)*.

——— (2011), *Thinking, Fast and Slow*, New York: Farrar, Straus and Giroux.

Klein, Gary (1998), *Sources of Power: How People Make Decisions*, Cambridge, Mass.: MIT Press.

Kulick, Jonathan, and Paul K. Davis (2003), *Modeling Adversaries and Related Cognitive Biases,* Santa Monica, Calif.: RAND Corp., RP-1084.

Mearsheimer, John (1983), *Conventional Deterrence*, Ithaca, N.Y.: Cornell University Press.

Morgan, Patrick M. (1983), "Deterrence: a Conceptual Analysis, 2d. ed.,".

——— (2003), *Deterrence Now*, London: Cambridge University Press.

Morral, Andrew R., and Brian A. Jackson (2009), *Understanding the Role of Deterrence in Counterterrorism Security,* OP-281-RC, Santa Monica, Calif.: RAND Corp.

National Research Council (2013), *Making Sense of Ballistic Missile Defense*, Washington, D.C.: National

Academies Press.
Naval Studies Board, and National Research Council (1996), *Post-cold War Conflict Deterrence*, Washington, D.C.: National Academy Press.
Perry, William J., Charles M. Vest, and Committee (2008), *Protecting Individual Privacy in the Struggle Against Terrorists: a Framework for Program Assessment*, Washington, D.C.: The National Academies Press.
Post, Jerrold M., ed. (2008), *The Psychological Assessment of Political Leaders*, Ann Arbor, Mich.: University of Michigan Press.
Rumsfeld, Donald (1998), *Executive Summary of the Report of the Commission to Assess the Ballistic Missile Threat to the United States*.
——— (2001), *Report of the Quadrennial Defense Review,* Washington, D.C.: Department of Defense.
Sanger, David E., and Charlie Savage (2013), "Obama is Urged to Sharply Curb N.s.a. Data Mining," *New York Times*, December 19, p. A1.
Sawyer, John (forthcoming) "Dissuasion by Denial in Counterterrorism: Theoretical and Empirical Deficiencies," in Andreas Wenger, and Alex Wilner, eds., *Deterrence by Denial: Theory, Practice, and Empiricism*, p.
Schneider, Barry R., and Jerrold M. Post, eds. (2004), *Know Thy Enemy: Profiles of Adversary Leaders and Their Strategic Cultures*, Washington, D.C.: U.S. Government Printing Office.
Sessler, Andrew M., John M. Cornwall, Bob Dietz, Steve Fetter, Sherman Frankel, Richard L. Garwing, Kurt Gottfried, Lisbeth Gronlund, George N. Lewis, Theodore A. Postol, and David C. Wright (2000), *Countermeasures: A Technical Evaluation of the Operational Effectiveness of the Planned Us National Missile Defense System,* Cambridge, Mass.: Union of Concerned Scientists and MIT Security Studies Program.
Simon, Herbert A. (1978) "Rational Decision-making in Business Organizations: Nobel Prize Lecture," in Assar Lindbeck, ed., *Nobel Lectures, Economics, 1969-1980*, Singapore: World Scientific Publishing Co., p.
Slovic, Paul, Baruch Fischoff, and Sarah Lichtenstein (1977), "Behavioral Decision Theory," *Annual Review of Psychology*, Vol. 28, pp. 1-39.
Snyder, Glenn H. (1960), "Deterrence and Power," *Journal of Conflict Resolution*, Vol. 4, No. 2, pp. 163-178.
Stein, Janice Gross (1991), "Reassurance in International Conflict Management," *Political Science Quarterly*, Vol. 106, No. 3, pp. 431-451.
Stein, Janice Gross, and Ron Levi (forthcoming) "The Social Psychology of Denial: Lessons from Crime Studies for Deterring Terrorism," in Alex Wilner, and Andreas Wenger, eds., *Deterrence by Denial: Next steps*, p.
U.S. Senate Armed Services Committee (2013), May 9, "Hearing to Receive Testimony on Ballistic Missile Defense Programs."
http://www.armed-services.senate.gov/imo/media/doc/13-40%20-%205-9-13.pdf
Ullman, Harlan K., and James P. Wade (1996), *Shock and Awe: Achieving Rapid Dominance*, Washington, D.C.: National Defense University Press.
USSTRATCOM (2010), *Exploring the Use of Alternative Analytical Techniques to Better Assess the Changing Roles of Nuclear Weapons in the Global Deterrence/assurance Dynamics: Terms of Reference (Draft),* Omaha, Neb.: U.S. STRATCOM.
Warrick, Joby, and Karen DeYoung (2013), "On Iran, Senators Defy White House. Threaten New Sanctions," *Washington Post*, December 19, p. online.
Washington Post (2001), "Bin Laden Discusses Attacks on Tape," *Washington Post*, December 13.
Woods, Kevin M. (2008), *The Mother of All Battles: Saddam Hussein's Strategic Plan for the Persian Gulf War*, Newport, RI: Naval Institute Press.