Cognitive Defense:

Influencing the Target Choices of Less Sophisticated Threat Actors

Jesse Wasson & Christopher Bluesteen

Abstract

With the emergence of non-state threats and new operating environments since the end of the Cold War, the relevance of deterrence as a security tool has repeatedly been called into doubt. Modern adversaries often lack territory, militaries, economies, or even identities to threaten and retaliate against. Their motivations are diverse and they are increasingly selecting soft targets on the basis of opportunity. Governments can no longer be relied upon as they once were to deter attacks against the homeland, shifting the burden of deterrence downward to the private and public parties being targeted. Alternative approaches are needed that account for this fundamental change. Taking inspiration from criminology and behavioral economics, we identify ways in which cognitive biases can be manipulated to affect adversary target preferences and then explore how this approach can be used to aid defenders on the ground.

Suggested Citation

Wasson, Jesse and Bluesteen, Christopher. "Cognitive Defense: Influencing the Target Choices of Less Sophisticated Threat Actors." *Homeland Security Affairs* 13, Article 1 (April 2017). https://www.hsaj.org/articles/13770

Introduction

With the emergence of new threat actors since the end of the Cold War, the relevance of deterrence as a security tool has frequently been called into doubt. Unlike past foes, many modern adversaries lack territory, militaries, economies, or even identities against which to retaliate. Their motivations are often varied and actions uncoordinated, making it virtually impossible to dissuade them from ever attacking in the same sense the United States was able to deter the Soviet Union from direct military conflict. In addition, increasingly these actors are selecting soft targets opportunistically instead of harder, more symbolic targets with grander payoffs.

Just six months before the 2015 Paris attacks, a prominent French jihadist was quoted in the Islamic State magazine *Dar al-Islam* telling his followers to abandon symbolism: "My advice is to stop looking for specific targets. Hit everyone and everything."[1] Meanwhile homegrown violent extremists, frustrated by domestic political conditions and inspired by international movements, are lashing out increasingly at targets in their local communities without discrimination. An underappreciated consequence of these developments is that the burden of deterrence has shifted downward from government to the private and public parties being targeted. The relevant question for security practitioners now is no longer whether there will be an attack, but who will be attacked. Alternative approaches to deterrence are needed that account for this fundamental change.

This article attempts to advance homeland security research by integrating findings from national security, criminological, and psychological disciplines to improve our understanding of deterrence at the target level. In doing so, it offers defenders on the ground practical ideas for how cognitive biases can be exploited to influence adversary preferences. The forthcoming sections review the deterrence literature from a variety of perspectives. We follow up with an analysis of theoretical gaps and the development of a framework to fill these gaps. Finally, we present the implications of these findings with various notional examples to demonstrate their application in the real world.

Background

The contemporary deterrence literature is vast, spanning nearly three quarters of a century and multiple disciplines. In the international and national security fields, early research sought ways to prevent nuclear war between the United States and Soviet Union. Consequently, most view deterrence from the strategic perspective of a unitary, rational government and assert that challenges to the status quo can best be thwarted by removing an adversary's motivation to act.[2] Some have criticized this line of thinking for relying on unrealistic notions of rationality and lacking empirical support.[3] Others have also challenged classical theory by exploring alternative models of decision making.[4] But the absolute prevention of conflict between rational state actors has continued to remain the dominant paradigm in both academic and policy circles.

Perhaps because of this, many have questioned the effectiveness of trying to deter the threat from modern terrorist entities which seem insatiable, lack territory or identity, and appear neither unitary nor rational.[5] The 2002 *National Security Strategy of the United States* embodied this view when it stated: "Traditional concepts of deterrence will not work against a terrorist enemy whose avowed tactics are wanton destruction and the targeting of innocents; whose so-called soldiers seek martyrdom in death and whose most potent protection is statelessness."[6] What the document advocated instead was a counterterrorism strategy designed to *defeat*, *deny*, *diminish* and *defend*—the word *deter* didn't even appear in the final version of the *2003 National Strategy for Counterterrorism* despite being a principal objective in earlier drafts.[7]

Others have argued, however, that while it might be difficult to deter terrorists, longstanding deterrence principles such as *punishment* and *denial* can be applied to these non-state actors.[8] The idea is that even if one cannot directly affect their motivation to act, one can still influence terrorists in the same manner as a state by threatening their capability to act (e.g., bases, finances, and sponsors). Moreover, one can deny them the benefits of action by hardening targets, downplaying effects, or communicating the target society's resolve. The Department of Defense's *2006 Quadrennial Defense Review* explicitly acknowledged a need to customize deterrence depending on the threat by introducing the concept of "tailored deterrence."[9]

Irrespective of these opposing conclusions, most skeptics and supporters of deterrence typically rely on the same classical deterrence mindset to understand how these new threat actors can or cannot be influenced, and by doing so they also subsume the same strategic imperative of absolute prevention of attack.[10] Deterrence skeptics see adversaries that are highly motivated, lack territory, and appear neither unitary nor rational and wonders how they could possibly be deterred in the same manner as past adversaries like the Soviet Union from ever attacking. Deterrence supporters see actors that, while in some ways are different from enemies of old, generally remain susceptible to the very same principles thought to achieve strategic deterrence previously. Scholars tend not to approach the problem in a fundamentally different way, but there are exceptions.

James Smith,Brent Talbot, Andrew Morral, and Brian Jackson do depart from this implicit goal of strategic deterrence (i.e., deterring attacks completely) to contemplate deterrence at tactical and operational levels of analysis.[11] Coming at the problem from a homeland security perspective as opposed to international strategy, they examine how terrorists might be deterred once the decision to attack has already been made. In doing so they consider methods for how individual attacks can be displaced onto less critical targets. Other lesser known works,[12] whose conceptualization of deterrence better resembles law enforcement's than the Pentagon's, become more important once the strategic imperative is dropped and attention turns to winning at the target level.

Collectively, these exceptions represent a category of deterrence that might be called "non-strategic" for they are concerned not with the absolute prevention of attack but rather the prevention of attack at specific locations. That being said, non-strategic deterrence should not be thought of as completely independent of strategic deterrence but rather complementary, at least when it comes to terrorism. For example, Doron Almog's theory of "cumulative deterrence" based on the Israeli experience asserts that repeated tactical and operational victories can, over time, deter an enemy strategically.[13]

Research at the non-strategic level, while a significant improvement in understanding how deterrence can be used effectively against non-state actors, does not address sufficiently a certain theoretical movement that has received increasing attention within the fields of public law and criminology. Although these disciplines are similarly rooted in strategic perspectives and rational choice models of decision making,[14] researchers have begun to question the validity of this, pointing to contrary evidence and findings from behavioral economics, a social psychological approach which rejects traditional *homo economicus* models of decision making, and which shows how biases in human cognition often cause systematic deviations from optimal choices.[15] These critics contend that while the general threat of punishment by governments may have some deterrent power, specific policies likely do not unless they deliberately account for cognitive biases. Criminology research at the non-strategic or target level echoes these concerns, suggesting that behavioral models, for instance, are superior to rational choice models in explaining the target preferences of burglars.[16]

For those interested in resuscitating deterrence to combat modern security threats such as terrorist groups and homegrown violent extremists, research at the non-strategic level of analysis is a step in the right direction. This work, however, remains hindered by an overreliance on orthodox notions of decision making and a disproportionate focus on the role of government as opposed to the actual defenders of targets. Much can be learned by applying behavioral economics principles in non-strategic contexts. But before doing so, it is first necessary to understand how differences in decision making between threat actors can affect deterrence.

Decision Making and Deterrence

The universal goal of deterrence is to influence decision making so that individuals, groups, or states choose not to take actions deemed undesirable by the deterrer.[17] Doing this requires manipulating one of two underlying factors required to act: motivation and opportunity.[18] Motivation is the reason why an actor seeks out a particular course of action. Opportunity is the actor's belief that he possesses the necessary *knowledge* and *capability* to successfully carry out that action. Knowledge represents awareness of targets that could satisfy motivations.[19] Capability refers to technical skills, equipment, weaponry, etc. estimated to have reasonable chance at success. For example, a destitute father responsible for the welfare of his children may be motivated to rob a convenience store because he needs to feed his family. However, failing to know the location of any nearby stores (knowledge) or not having a weapon (capability) may preclude the robbery due to a lack of opportunity. Conversely, a wealthy man with a concealed weapon standing outside a deserted gas station is not likely to consider theft for lack of any compelling motivation. Each of these factors is a point of influence a deterrer could potentially exploit to achieve deterrence.

While motivation and opportunity are the core elements of decision making, their relative importance for deterrence depends on the threat actor's level of sophistication. All actors are not created equal when it comes to their susceptibility to manipulation. More sophisticated actors, such as states or advanced terrorist groups (e.g., Hezbollah) are less likely to be influenced by intentional distortions of knowledge (e.g., decreasing a target's visibility) or inflated capability demands (e.g., increasing a target's defenses) because the financial, technical, and organizational resources available to them can be used to overcome attempts to deny them opportunity. Of all types of potential threat actors, the knowledge of these sophisticated actors comes closest to perfect information and their capabilities are hardest to mitigate, which is why they can deliberately select harder targets with larger payoffs. Ironically, though, actors of greater means are more sensitive to deterrer actions which negatively impact their motivation (e.g., military strikes, economic sanctions) because they have much to retaliate against. Moreover, because of their ability to seriously hurt their adversaries, these actors are more likely to receive positive inducements (i.e., incentives that encourage restraint) in exchange for refraining from acting.

For instance, U.S. deterrence policy against the Soviet Union during the Cold War centered on influencing Soviet motivations through cost imposition (e.g., flexible response) and positive inducements (e.g., removing Jupiter missiles from Turkey). In later years, U.S. strategy also broadened to include programs such as missile defense that challenged the Soviet capability to execute a successfully attack, even though the effectiveness of these programs was, and still is, dubious. Due to their advanced intelligence network and deliberate decision making process, however, the U.S. never really pursued the knowledge element of opportunity. Although a campaign aimed at influencing Soviet perceptions of critical American targets may have seen short-term success, U.S. leadership likely assumed it would ultimately fail as the Soviets eventually gravitated toward optimal actions based on information that came closer and closer to reality.

In contrast, less sophisticated threat actors such as domestic terrorists, homegrown violent extremists, or criminals have few if any resources to retaliate against and are less likely to be presented with acceptable alternative courses of action given their relative inability to hurt governments. Consequently, they have relatively little to lose by acting and are unlikely to be as responsive as more sophisticated actors to attempts to manipulate their motivation. These actors are, however, highly susceptible to efforts which seek to deny them opportunity since they lack the resources necessary to allay distortions of knowledge and inflated capability demands. Of all potential threat actors, their knowledge is farthest from perfect information and their capabilities easiest to mitigate, which is why they are more likely to select softer targets with smaller payoffs.

For example, in an interview shortly before his execution in 2001, Timothy McVeigh explained why he chose the Alfred P. Murah federal building for his 1995 attack: "I didn't have the ability to scope out every federal building in the nation. But I did scope out a number so I could pick the best out among those. The building was chosen out of a phonebook, looking in the blue pages, and looking under law enforcement agencies."[20] Moreover, because these actors do not necessarily need to attack one target in particular, they may select capriciously rather than employing a strict cost/benefit calculation. David Headley, for instance, when describing why he surveilled the Oberoi-Trident Hotel in Mumbai for the 2008 Lashkar-i-Taiba terrorist attacks stated: "[b]ecause I was in the area, and I was going to watch a movie in a nearby theatre, and I had about an hour left. So I went there, and I just made the video."[21] Finally, criminology studies show that burglars, including more experienced perpetrators, frequently select targets based on immediate opportunity.[22]

In each of these examples, the actor's motivation to attack was already hardened and apparently unaffected by government efforts to deter them. Strategic deterrence had failed; someone was going to be targeted. Rational choice-based models tend to assume all decision makers then maximize utility by picking the best target among the universe of all possible options. While this may be a reasonable assumption for more sophisticated actors, it does not appear to be the case at least for some less sophisticated actors. Instead, targets are selected within a constrained set of choices to satisfy minimal knowledge and capability requirements. And why one is selected over another has less to do with maximizing utility than the threat actor's casual *perceptions* of opportunity.[23] Next we will explore the theoretical and empirical justification for this reasoning, as well as how it expands the tools available to defenders at the target level.

Target Selection and Cognitive Biases

To achieve deterrence, information must be communicated to potential adversaries that convinces them not to act. In the strategic context, this typically occurs in the form of verbal threats of punishment or shows of force by governments. In the non-strategic context, it is usually just a byproduct of a target's security measures intended to defeat or mitigate attacks should deterrence fail as opposed to proactive efforts by a defender to prevent an attack in the first place. For example, federal buildings may have guards to interdict and neutralize potential attacks with the assumption that such actions also have some residual impact on deterrence attacks by communicating an increased cost of action. Although there are security systems which are designed first and foremost with deterrence in mind, [24] a high correlation between defeat and deter measures generally inhibits the development of systems much beyond guns, gates, and guards.

This assumption that defensive actions have some degree of positive impact on deterrence is almost certainly true so long as they are visible or otherwise perceived by the adversary. However, such a view of deterrence fails to appreciate the full spectrum of actions the defender of a target may take to deter less sophisticated threat actors. The means to deter can also include the deliberate manipulation or concealment of information pertaining to the capabilities required to act or the target's associated payoff. These more unconventional forms of deterrence may influence the preferences of potential threat actors just as do conventional forms, the only difference being in the former case the actor might not even realize they have been deterred.

How can this be done? Non-strategic deterrence success requires only that a specific target not be attacked. This can be accomplished in one of two ways: either the target is considered but not selected or the target is never considered in the first place. The former suggests that if perceived capability demands and payoffs can be shaped so that a potential actor discounts a target they otherwise would have preferred relative to all others, deterrence will have been achieved. The latter suggests that if the perceived viability or existence of a target can be altered so that a potential actor fails to consider the otherwise desirable target at all, deterrence will have been achieved. Defenders of targets, unlike governments, are in an advantageous position where they control much of the information from which values and choices are derived and can use it to influence surreptitiously threat actor perceptions. Viewed this way, non-strategic deterrence becomes less about directly affecting decisions than about shaping preferences and the development of choices governing those decisions—something better explained by psychology and behavioral economics than rational choice.

The theoretical and empirical support for this proposition is rooted in the idea of bounded rationality. According to this view, decision making is more accurately modeled as an intrinsic process of satisficing by which a choice is made amongst a constrained set of options on the basis of whether it is merely good enough rather than a deliberate process of utility maximization amongst an idealized set of options, as often modeled by rational choice theorists.[25] All actors, but particularly those less sophisticated who have fewer materiel and cognitive resources, lack perfect information regarding the existence, benefits, and costs of every possible target and do not make decisions with a god-like objective calculus. Some 60 years ago in introducing bounded rationality, Herbert Simon asserted: “[i]t is precisely because of these limitations on its [the organism’s] knowledge and capabilities that the less global models of rationality described here are significant and useful.”[26] The same can be said for deterrence today. Using a more realistic model of decision making based on bounded rationality may reveal previously unknown unconventional means to deter.

While bounded rationality provides the underlying model, deciphering its significance for non-strategic deterrence requires understanding the psychology of human cognition. Daniel Kahneman explains the major cognitive processes generally agreed to be operating: System 1 (Intuition) is passionate, reflexive, involuntary, and hard to change; while System 2 (Reasoning) is purposeful, conscientious, and malleable.[27] According to Kahneman, “the perceptual system and intuitive operations of System 1 generate *impressions* of the attributes of objects of perception and thought. These impressions are not voluntary and need not be verbally explicit. In contrast, *judgments* are always explicit and intentional, whether or not they are overtly expressed.”[28] He further describes System 1 as “effortlessly originating impressions and feelings that are the main sources of the explicit beliefs and deliberate choices of System 2.”[29] These systems usually perform quite well and allow humans to make sound decisions quickly; however, System 1 has two traits that can cause problems-- it has systematic biases and cannot be turned off.[30]

Given the materiel and cognitive resources of more sophisticated threat actors, including their likely use of command and control systems for decision making, it is fair to assume these groups “think slower” with cognition weighted more heavily toward System 2 than System 1.[31] With relatively fewer resources and little to no formal decision making bureaucracy, less sophisticated actors, on the other hand, undoubtedly “think faster” with cognition weighted more heavily toward System 1 than System 2. An important question then for non-strategic deterrence is what are the biases associated with System 1 and can they be used to deter less sophisticated adversaries? There is a substantial body of empirical research in psychology that has identified numerous System 1 biases.[32] More than just an academic curiosity, these biases have been known and exploited by the advertising industry for decades, and as mentioned previously, have recently begun to infuse behavioral economic approaches to public and criminal law, health, finance, etc.[33] Though there are perhaps hundreds of different biases, only a subset of the major categories will be explored here.

The first of these is *accessibility*. Because human beings are unable to collect and recall every piece of relevant information for any particular activity, only those thoughts which are perceived and accessible will ever be evaluated. Some information will simply never be perceived because of time and resource constraints. Other information, while perceived, may not be readily accessible due to biases in System 1. For example, ingrained predispositions to avoid certain negative stimuli, physical salience, and strong emotions can all influence accessibility on a subconscious level. This inability to perceive all relevant information together with System 1 prejudices creates a selection effect in which choices available to an actor do not represent the true population but rather a truncated sample. If as Kahneman says, "[h]ighly accessible features will influence decisions, while features of low accessibility will largely be ignored,…" defenders may be able to manipulate perceptions in order to bias that sample in their favor so that a target or its features are more/less likely to be accessed by an adversary when it comes time to make a decision.[34]

A second and related category of bias is *availability*. Availability has to do with how people estimate the frequency or probability of something. Instead of making objective evaluations on the basis of fact, humans tend to give greater weight to those impressions that are more readily available mentally. Recent occurrences, continual media attention, personal experience, negative emotions, salience, and associate bonds can all work on System 1 to distort reality. For instance, experiments have suggested that certain facial features (e.g., eyes color/shape, facial width-to-height rations) can lead people to misjudge temperament due to prejudices of availability, despite evidence to the contrary. Defenders that understand these biases may be able to increase deterrence by seeking to maximize or minimize "availability" of a target or its features.

The third category of bias, *representativeness*, refers to the propensity of the human mind to evaluate the probability or value of something based on its similarity to an archetype (prototype heuristics) as opposed to using base-rates and accounting for uncertainty. Studies have demonstrated corollaries of this bias in violations of monotonicity and dominance.[35] For example, individuals will assign higher values to sets of sports cards that do not include extra, less desirable cards despite being exactly the same.[36] In addition, patients will report preferring longer colonoscopies to shorter ones provided they do not end in pain.[37] Tangential to representativeness is self-affirmation theory, which explains how people respond to threats against their perceived notions of self-integrity.[38] Experiments, for instance, have shown that using self-relevant nouns like "cheater" in instructions, as opposed to "cheating," significantly reduces rates of dishonest behavior.[39] It is possible defenders could exploit representativeness in order to deter threat actors non-strategically by playing on their System 1 tendencies to make erroneous assessments on the basis of stereotypes, misremembered utilities, and distorted self-images.

Related to representativeness is a fourth category of bias, *relativity*. Relativity biases arise because human beings do not make absolute value judgments but instead assess everything relative to something else. A number of specific biases can be thought of as associated with relativity including anchoring, the decoy effect, and framing. It is also a foundational principle of prospect theory which asserts that utility is experienced as change from a neutral reference point.[40] Evidence in support of relativity-based biases is abound.

For instance, studies have shown that people over (under) estimate the probability of conjunctive (disjunctive) events because their estimates are anchored on the probability of the components which are relatively higher (lower).[41] Manufacturers often create decoy product models solely for the purposes of pushing consumers towards another model.[42] Finally, experiments have called into question the stability of people's preferences by showing that they can be highly dependent on whether information is framed positively or negatively.[43] By shaping how information is presented, defenders may be able to take advantage of a threat actor's relativity bias so that it induces a greater deterrent impact.

The aforementioned biases are just some of the ways System 1 can cause human beings to systematically deviate from what might objectively be considered optimal behavior. There are many others that may be relevant for deterrence such as hyperbolic discounting, illusion of control, and even optical illusions. Thus, a behavioral economics approach to non-strategic deterrence reveals additional means to prevent attack that have been previously overlooked. Because the decisions of less sophisticated threat actors are boundedly rational and defenders control critical inputs used to make those decisions, there is a tremendous amount of latent deterrence untapped by conventional security measures.

Application

With the theoretical implications established, it is now possible to contemplate notional illustrations of how defenders may influence the target choices of less sophisticated threat actors by exploiting their cognitive biases. The best way to do this is to think of deterrence as a force that either pushes a potential attacker away from a target of interest or pulls them towards it. *Push* is desirable and is realized by communicating high costs of action or low benefits of action. *Pull* is undesirable and comes about by communicating low costs of action or high benefits of action. The goal of non-strategic deterrence is to effectively manipulate these levers to the advantage of the defender. Critical infrastructure owners and protectors can exercise both push and pull by communicating information to potential attackers through visual or audio cues (e.g., signs, personnel, building facades, loudspeakers) and old media (e.g., television, radio, and print) but also new mediums such as social networks (e.g., Facebook, Twitter) and websites. In fact, new media have created an unprecedented opening for defenders to influence less sophisticated threat actors due to their likely reliance on such media as a cheap source of target information.

The means of deterrence used to push or pull adversaries can be conventional or unconventional. Undoubtedly, defeat measures which also happen to provide some degree of deterrent benefit account for a disproportionate amount of the deterrence for most defenders. However, these are often expensive and fail to capitalize on the potential opportunities afforded by taking advantage of the less expensive and more unconventional means discussed previously. The following offers some preliminary ideas for how cognitive biases might be manipulated to achieve non-strategic deterrence.

The targets of less sophisticated threat actors vary as widely as the manner in which they are protected. A store may do nothing to defend itself against criminals apart from locking the register, whereas a government building fearing terrorism may have armed guards, cameras, and anti-vehicle barriers. All these measures likely have some deterrent effect by pushing an actor away from a target provided they perceive the costs of attack, but this is not always the case. Defenders may simply fail to appreciate the significance of communicating costs or conceal defensive capabilities deliberately so potential threat actors are unaware of the specific skills and equipment required to defeat the system. For example, while defense in depth security strategies may be optimal, they project lower costs of attack at the perimeter than is actually the case overall. To compensate for this, defenders should consider the value of overt security patrols and interactions with the community, regardless of their limited tactical benefit. Websites and other media too may be helpful for communicating criminal penalties or the use of deadly force should attacks be attempted. And for those concerned about defeat, signs describing the security system can be employed to emphasize the costs of action without having to divulge compromising information. The more easily costs are available and accessible by threat actors mentally when it comes time to consider and select targets, the more likely deterrence will succeed.

Defenders may likewise fail to appreciate the significance of communicating low benefits to push threat actors away, although coming up with practical ideas is not as easy as one might think. The most obvious example, of course, is the use of signs by stores or banks to indicate limited cash available. Defenders could also conceivably lie about benefits to lower perceptions, which might be advisable if it is legal and the consequences of being found out do not undermine the original intention. A more realistic example, however, could be potential targets such as power plants and distribution systems going out of their way to publicize that an attack on their facilities would not cause widespread damage due to equipment and network redundancies. Resiliency must be plainly obvious to attackers if it is to have any influence on their perceptions of whether the target is a viable opportunity.

Just as important as what information is conveyed about the high costs and low benefits of action, is how that information is conveyed. Well-understood techniques from advertising can help increase the chances that information regarding the costs of action presented through social networks, websites, or visual cues is readily available, accessible, and relative in the minds of potential threat actors. For instance, defenders should frame information in a manner which expresses the losses actors would experience as opposed to the effectiveness of the security system. Words may be less powerful than certain colored imagery that conveys a willingness to employ violence against attackers and evokes feelings of fear. The inclusion of subtle, negative stimuli (e.g., suspicious looking eyes) that elicit primitive emotional responses of fear could be used as well to inflate the costs of action perceived. Other techniques might include contrasting security features with generic targets that are less secure and present a greater payoff.

In addition to availability, accessibility, and relativity biases, manipulating representativeness biases associated with the costs of action could also be effective. Ensuring that security guards and spokesman most likely to come in contact with the public look "more like security" and have facial features known to stimulate negative reactions may increase the perception of high costs. Providing these individuals with equipment (e.g., tactical vests) which that may not be operationally relevant but which promote an illusion of validity could help to reinforce this perception. Furthermore, the mindful placement of warning signs, guards, etc. near exits to ensure they are the last stimuli received by threat actors before departing a target location might have a disproportionate effect on how costs are remembered. Lastly, publicizing the consequences of failed attacks at other similar locations could influence adversary perceptions of the target's net value.

The converse to these means which push adversaries away is minimizing information which pulls them in (i.e., low costs of action or high benefits of action). The simplest way to do this is to reduce the amount of potentially attractive information released or portrayed to the public so that it is less available and mentally accessible by threat actors when it comes time to consider and select targets. Examples might include masking vulnerabilities that cannot be mitigated, conducting sensitive operations at night, and ensuring that staging/ queuing locations are not easily observable by the public. In addition, enforcing strict media blackouts on minor security incidents or near-misses may help avoid attracting attention from potential attackers who may have previously been unaware of the target.

An even more powerful device, given our reliance on the internet as a source of information, is search engine "de-optimization". Much like online reputation management services use tools to diminish the rank of embarrassing links in search results or remove unflattering information entirely, defenders can do the same thing to decrease (or increase) the likelihood that certain information is seen by threat actors (e.g., via robots.txt files). Defenders can do this much more easily considering they own or can edit many of the websites of interest. For example, defenders can diminish the rank of search results pertaining to a target's payoffs while at the same time inflating the rank of information related to security features. Even more popular targets for which the "cat is already out of the bag" in terms of payoff can be counter-balanced by higher ranking information that reduces pull or increases push.

Although the concept of push and pull is most directly applicable to defenders of discrete targets, it may also be useful for government agencies or corporations responsible for a portfolio of potential targets. The Department of Homeland Security, for instance, is charged with assessing risk and allocating resources for assets across the United States. They, like many, usually define risk as a function of *threat*, *vulnerability*, and *consequence* or (TVC).[44] Where *threat* is the probability of attack, *vulnerability* is the probability the attack succeeds should it occur, and *consequence* is the impact of successful attack. There are numerous problems, however, with using such a framework to assess risk including the inability to measure threat, limited notions of what constitutes vulnerability, and correlated or interdependent terms.[45] Alternative models have been proposed that alleviate some of these issues by either ignoring the threat component altogether and focusing instead on vulnerability, or treating threat as an output of the adversary's expected utility calculation based in part on their capabilities to defeat a target.[46]

None of these approaches address the knowledge element of opportunity emphasized throughout this article, and therefore, they do not account for associated biases that likely impact adversary target selection. The less sophisticated the actor, the less likely it is that they maximize opportunity by selecting the best target off the full menu according to vulnerability and consequence, and the more likely it is that they simply satisfice within a local subset. Evidence indicates terrorists and criminals usually choose targets that are geographically close or familiar due to, among other things, their limited ability to project power and propensity to seek immediate gratification.[47] Assuming defenders of targets with similar payoffs take roughly equal actions to deter attacks, the nature of the local environment will influence the level of push and pull perceived by the threat actor.

For example, all things being equal, a government building or transportation hub that does not have equivalent targets nearby is likely to exude greater pull than one that resides in an environment with a plethora of substitute targets. Critical infrastructure found on a busy street downtown will probably exude greater push than an equally well known sister site found in an industrial park on the outskirts of town. In other words, an absolute level of push and pull is less relevant than the relative levels associated with proximate targets. As a result, the risk of attack would be more accurately assessed through a lens that normalizes relative levels of push and pull across similar targets within the local environment. Governments and corporations should at least consider this effect when determining how to best allocate resources across their enterprise.

Conclusion

To account for new challenges that existing theories have struggled to address, we presented an alternative view of deterrence here featuring a behavioral approach to preventing attacks at the target level. It is applicable to terrorist and criminal actors alike and offers defenders new tools that go well beyond basic operational security. While we have made a number of contributions to homeland security research, one important question remains unanswered. How much do the hypothesized unconventional means of deterrence impact target selection and preferences? Though the cognitive biases referenced have received strong empirical support in psychology and behavioral economics, their non-strategic deterrence applications have yet to be directly tested. Doing so is the obvious next step but this will be challenging given the phenomena in question and available data.

The global proliferation of terrorism has increasingly threatened public and private parties that cannot employ advanced security either because of its expense or operational impact. The 2015 Paris attacks were carried out by a moderately sophisticated threat actor against a variety of soft targets including a football stadium, two bars, four restaurants, and a concert hall. The tragic result was 130 people killed and hundreds wounded. For the city of Paris and the French government it was an all too common, and perhaps unavoidable, failure of strategic deterrence. For the many establishments targeted, it was a failure of non-strategic deterrence.

For equivalent locations that were not chosen by the attackers, however, deterrence succeeded. Perhaps this was because they had sufficient security to dissuade the attackers or offered relatively smaller payoffs. Perhaps it was because they simply appeared more secure and less valuable, or didn’t appear at all. The upshot is that public and private parties are not completely powerless in the fight against terrorism—they have the ability to influence the target choices of threat actors in their favor. A shrewder approach to deterrence based on the principles described herein could provide significant improvements in overall security for relatively little cost.

About the Authors

Jesse T. Wasson is a Senior Policy Analyst at Systems Planning and Analysis in Alexandria, Virginia where he primarily focuses on threat assessment, security risk, and organizational performance for the U.S. Navy, National Nuclear Security Administration, and private sector clients. Dr. Wasson holds a Ph.D. in political science from the State University of New York at Buffalo and was formerly a visiting assistant professor of political science at the Rochester Institute of Technology. He can be reached at jwasson@spa.com.

Christopher E. Bluesteen is a Senior Security Analyst at Systems Planning and Analysis in Alexandria, Virginia where he focuses on vulnerability assessment and risk management for the U.S. Navy, National Nuclear Security Administration, the Office of the Secretary of Defense, and private sector clients. Prior to this, Mr. Bluesteen served as an Armor Officer in the U.S. Army. Mr. Bluesteen holds a B.S. in computer engineering from The College of New Jersey and a M.S. in operations research from George Mason University. He can be reached at cbluesteen@spa.com.

Notes

[1] Rukmini Callimachi, Alissa J. Rubin, and Laurie Fourquet, “A View of ISIS’s Evolution in New Details of Paris Attacks,” *New York Times*, March 19, 2016.

[2] Notable examples include William Kaufmann, “The Requirements of Deterrence,” in William Kaufmann (ed.), *Military Policy and National Security* (Princeton: Princeton University Press, 1956); Daniel Ellsberg, “The Theory and Practice of Blackmail” (Lecture at the Lowell Institute, Boston, March 10, 1959); Herman Kahn, *On Thermonuclear War* (Princeton: Princeton University Press, 1960); Thomas C. Schelling, *The Strategy of Conflict* (Cambridge: Harvard University Press, 1960); Glenn H. Snyder, *Deterrence and Defense* (Princeton: Princeton University Press, 1961).

[3] Alexander L. George and Richard Smoke, *Deterrence in American Foreign Policy: Theory and Practice* (New York: Columbia University Press, 1974); Ole Holsti and Alexander L. George, “The Effects of Stress on the Performance of Foreign-Policy Makers,” in Cornelius Cotter (ed.) *Political Science Annual, VI* (Indianapolis: Bobbs-Merril, 1975); Patrick Morgan, *Deterrence: A Conceptual Analysis* (Beverly Hills, CA: Sage, 1977); Glenn H. Snyder and Paul Diesing, *Conflict Among Nations* (Princeton: Princeton University Press, 1977); Robert Jervis, “Deterrence Theory Revisited,” *World Politics* 31, no. 2 (1979).

[4] Robert Jervis, Richard Ned Lebow, and Janice Gross Stein, *Psychology and Deterrence* (Baltimore: The Johns Hopkins University Press, 1985); Keith B Payne, *The Fallacies of Cold War Deterrence and a New Direction* (Lexington, KY: University Press of Kentucky, 2001); Jeffrey D. Berejikian, “A Cognitive Theory of Deterrence,” *Journal of Peace Research* 39, no. 2 (2002); Gary Schaub Jr., “Deterrence, Compellence, and Prospect Theory,” *Political Psychology* 25, no. 3 (2004).

[5] Paul K. Davis and Brain Michael Jenkins, *Deterrence and Influence in Counterterrorism: A Component in the War on al Qaeda* (Santa Monica, CA: RAND Corp, 2002); Richard K. Betts, “The Soft Underbelly of American Primacy: Tactical Advantages of Terror,” *Political Science Quarterly* 117, no. 1 (2002); Colin S. Gray, “Maintaining Effective Deterrence,” Strategic Studies Institute (US Army War College, 2003).

[6] Available at http://www.state.gov/documents/organization/63562.pdf.

[7] Doron Almog, “Cumulative Deterrence and the War on Terrorism,” *Parameters*, 34, no. 4 (2004): 15. The word “deter” does appear in the *2011 National Strategy for Counterterrorism*, though it is not an overarching goal.

[8] Robert Trager and Dessislava Zagorcheva, “Deterring Terrorism: It Can Be Done,” *International Security*, 30, no. 3 (2005); Matthew Kroenig and Barry Pavel, “How to Deter Terrorism,” *The Washington Quarterly*, (Spring 2012).

[9] Available at http://archive.defense.gov/pubs/pdfs/QDR20060203.pdf.

[10] Due to the extremely high costs of nuclear war, it is understandable that contemporary deterrence theory began with a focus on the absolute prevention of conflict. Applying that same standard to newer adversaries that cannot existentially threaten the deterrer, however, is unnecessarily limiting theoretically. See Jeffrey W. Knopf, “The Fourth Wave in Deterrence Research,” *Contemporary Security Policy*, 31, no. 1 (2010).

[11] James M. Smith and Brent J. Talbot, “Terrorism and Deterrence by Denial,” in Paul R. Viotti, Michael A. Opheim, and Nicholas Bowen (eds.), *Terrorism and Homeland Security* (Boca Raton, FL: CRC Press, 2008); Andrew R. Morral and Brian A Jackson, *Understanding the Role of Deterrence in Counterterrorism Security* (Santa Monica, CA: RAND Corp., 2009).

[12] Robert W. Anthony, *Deterrence and the 9-11 Terrorists* (Alexandria, Virginia: Institute for Defense Analyses, 2003); Tom LaTourrette et al. , *Reducing Terrorism Risk at Shopping Centers* (Santa Monica, CA: RAND Corp, 2006); James H. Lebovic, “Deterrence and Homeland Security: A Defensive-Denial Strategy Against Terrorists,” in Esther Brimmer (ed.), *Five Dimensions of Homeland and International Security* (Washington, DC: Center for Transatlantic Relations, John Hopkins University, 2008); Konstantinos G. Gkonis, Harilaos N. Psaraftis, and Nikolaos P. Ventikos, “Game Theory Contributing to Terrorism Analysis in Merchant Shipping: An Application to Port Security,” Working Paper, National Technical University of Athens, 2009; Henry H Willis, Joel B. Predd, and Paul K Davis, *Measuring the Effectiveness of Border Security Between Ports-of-Entry* (Santa Monica, CA: RAND Corp, 2010).

13 Almog, "Cumulative Deterrence".

14 Gary S. Becker, *The Economic Approach to Human Behavior* (Chicago: University of Chicago Press, 1976).

15 Christine Jolls, Cass R. Sunstein, and Richard Thaler, "A Behavioral Approach to Law and Economics," *Stanford Law Review* 50 (1998); Paul H. Robinson and John M. Darley, "Does Criminal Law Deter? A Behavioral Investigation," *Oxford Journal of Legal Studies* 24, no. 2 (2004); Christine Jolls, "On Law Enforcement with Boundedly Rational Actors," Harvard Law and Economics Discussion Paper No. 494 (2004); Richard H. McAdams and Thomas S. Ulen, "Behavioral Criminal Law and Economics," University of Chicago Law & Economics, Olin Working Paper No. 440 (2008).

16 Paul F. Cromwell, James N. Olson, and D'Aunn W. Avary, *Breaking and Entering: An Ethnographic Analysis of Burglary* (Newbury Park, CA: Sage, 1991); Kristie R. Belvins, Joseph B. Kuhns, and Seungmug Lee, "Understanding Decisions to Burglarize from the Offender's Perspective," The University of North Carolina at Charlotte Department of Criminal Justice and Criminology (2012).

17 Deterrers may be governments or those responsible for defending discrete targets, though their goals differ. Governments are less concerned with deterring single attacks than they are in reducing their overall likelihood, since any one attack is a failure of deterrence. Defenders of discrete targets, on the other hand, care only about deterring attacks against themselves even if that means displacing attacks elsewhere.

18 Requiring theoretically that actors possess both motive and opportunity in order to act is hardly novel. The framework, or some variation thereof, is fundamental to criminology theories and has even been used at the nation-state level in the study of war. See for example Randolph M. Siverson and Harvey Starr, "Opportunity, Willingness, and the Diffusion of War," *American Political Science Review* 84, no. 1 (1990).

19 Despite its importance, *knowledge* is frequently overlooked or assumed away in most analyses of threat actor decision making because of how difficult it is to measure compared to *capability*.

20 Toby Oppenheimer, *The McVeigh Tapes: Confessions of an American Terrorist* (United States: MSNBC Films, April 19, 2010).

21 Sebastian Rotella, "The American Behind India's 9/11—And How U.S. Botched Changes to Stop Him," *ProPublica*, 2013, http://www.propublica.org/article/david-headley-homegrown-terrorist.

22 Cromwell et al., *Breaking and Entering* (note 13); Belvins et al., "Decisions to Burglarize."

23 Because the biggest factor influencing threat actors' target choice is likely their spatial constraints, perceptions of opportunity are relative within the immediate environment. Significant evidence points to the fact that crimes and terrorist attacks are usually conducted in locations that are geographically close or familiar to the perpetrators. For criminal examples, see Wim Bernasco and Paul Nieuwbeerta, "How do Residential Burglars Select Target Areas?" *British Journal of Criminology* 45, no. 3 (2005). For terrorism, see Nurit Kliot and Igal Charney, "The Geography of Suicide Terrorism in Israel," *GeoJournal* 66, no. 4 (2006); Claude Berrebi and Darius Lakdawalla, "How Does Terrorism Risk Vary Across Space and Time? An Analysis Based on the Israeli Experience," *Defense and Peace Economics* 18, no. 2 (2007).

24 Crime Prevention through Environmental Design (CPTED), for example, describes how the natural or constructed environment can be deliberately shaped to improve access control, surveillance, or other means to reduce the opportunity for criminal acts to occur. For a review of the literature see Matthew Robinson, "The Theoretical Development of CPTED: Twenty-five Years of Responses to C. Ray Jeffrey," in W. Laufer and F. Adler (eds.), *Advances in Criminological Theory*, *Vol. 8* (New Jersey: Transaction Publications, 1996).

25 Herbert Simon, "A Behavioral Model of Rational Choice," *The Quarterly Journal of Economics* 69, no. 1 (1955); Herbert Simon, "Rational Choice and the Structure of the Environment," *Psychological Review* 63, no. 2 (1956).

26 Simon, "A Behavioral Model," p. 112.

27 Daniel Kahneman, "Maps of Bounded Rationality: Psychology for Behavioral Economics," *The American Economic Review* 93, no. 5 (2003).

28 *Ibid.*, 1452.

29 Daniel Kahneman, *Thinking Fast and Slow* (New York: Farrar, Straus and Giroux, 2011), 21.

30 *Ibid.*, 25. Given practice and experience, System 1 biases can be partially, but not completely, mitigated by System 2.

31 This is not to suggest these actors are completely immune from bias. But they likely face a different set of decision-making biases (e.g., group think, non-transitive preferences) based on group dynamics as opposed to human cognition.

32 For detailed reviews of this research see Amos Tversky and Daniel Kahneman, "Judgment under Uncertainty," *Science* 185, no. 4157 (1974); Kahneman, "Bounded Rationality" (note 24); Kahneman, *Thinking Fast* (note 27); Dan Ariely, *Predictably Irrational* (New York: HarperCollins, 2008).

33 See for example Marc Andrews, Matthijs van Leeuwen, and Rick van Baaren, *Hidden Persuasion* (Amsterdam: BIS, 2013); Jolls, "On Law Enforcement" ; Richard H. Thaler and Cass R. Sunstein, *Nudge* (New Haven, CT: Yale University Press, 2008).

34 Kahneman, "Bounded Rationality," 1459.

35 *Ibid.*

36 John A. List, "Preference Reversals of a Different Kind: The 'More is Less' Phenomenon," *American Economic Review* 92, no. 5 (2002).

37 Donald A. Redelmeier and Daniel Kahneman, "Patients' Memories of Painful Medical Treatments: Real-time and Retrospective Evaluations of Two Minimally Invasive Procedures," *Pain* 66, no. 1 (1996).

38 David K. Sherman and Geoffrey L. Cohen, "The Psychology of Self-Defense: Self-Affirmation Theory," *Advances in Experimental Psychology* 38 (2006).

39 Christopher J. Bryan and Gabrielle S. Adams, "When Cheating Would Make You a Cheater: Implicating the Self Prevents Unethical Behavior," *Journal of Experimental Psychology* 142, no. 4 (2012).

40 Daniel Kahneman and Amos Tversky, "Prospect Theory: An Analysis of Decisions Under Risk," *Econometrica* 47, no. 2 (1979).

41 Tversky and Kahneman, "Judgment under Uncertainty," 1129.

42 Ariely, *Predictably Irrational* , 14-15.

43 Kahneman, *Thinking Fast*.

44 U.S. Department of Homeland Security, *Risk Management Fundamentals* (April 2011).

45 Louis A. Cox, "Some Limitations of 'Risk=Threat x Vulnerability x Consequence' for Risk Analysis of Terrorist Attacks," *Risk Analysis* 28, no. 6 (2008); National Research Council of the National Academies, *Review of the Department of Homeland's Security's Approach to Risk Analysis* (Washington, DC: The National Academies Press, 2010); Gerald G. Brown and Louis A. Cox, "How Probabilistic Risk Assessment Can Mislead Terrorism Risk Analysts," *Risk Analysis* 31, no. 2 (2011); Eric F. Taquechel and Ted G. Lewis, "How to Quantify Deterrence and Reduce Critical Infrastructure Risk," *Homeland Security Affairs* 8 (August 2012); Richard White, "Towards a Unified Homeland Security Strategy: An Asset Vulnerability Model," *Homeland Security Affairs* 10 (February 2014).

46 See White, "Homeland Security Strategy" and Taquechel and Lewis, "How to Quantify Deterrence", respectively.

47 See note 23.

Cover image by Mstyslav Chernov - Own work, CC BY-SA 4.0, https://commons.wikimedia.org/w/index.php?curid=45277301