



CENTER FOR TRANSATLANTIC RELATIONS

Deterrence and Homeland Security: A Defensive-Denial Strategy against Terrorists

James H. Lebovic

Terrorists are allegedly difficult to deter because they are hard to punish. But terrorists are *punished* when they are *denied* their objectives with defenses that cause an attack to fail. When their attacks fail, terrorists must accept costs (punishment) in the form of a lost capacity to attack alternative targets or the same target, at some future point, under more favorable conditions. The costs of failure are prohibitive when the success of an attack depends upon surprise and the defender is now on alert. Then, the "next" attack will be harder to engineer than the last. The costs of failure are also high when a current operation will expend valuable and, perhaps, irreplaceable offensive assets such as the trained commercial pilots that were essential to the September-11 attacks. Given these costs, terrorists might choose not to attack, might choose to attack a less consequential target, or might delay an attack giving the defender time to pick up signs that an attack is forthcoming and to prepare accordingly. *All three outcomes are desirable from a deterrence standpoint.*

What Targets Require Defending?

A defensive-denial strategy must respond to a simple question, "what targets require defending?" The answer is complicated, however, because a wealth of available attack choices permit terrorists to strike not just unusually vulnerable or valuable targets but especially vulnerable *and* valuable ones. For example, the exclusive screening of carry-on luggage at airports would allow terrorists to smuggle bombs onto planes in the cargo hold. The quandary for the defender is knowing what to protect, then, when it cannot protect everything. More specifically, the issue is what to select for protection and what to exclude from protection given two complications.

First, lesser defensive priorities are still inviting targets. In fact, it is hard to conceive of a target that offers at least some political dividends to a terrorist if attacked successfully that is not also valued by the targeted government or society. Thus, from the defender's perspective, everything appears vulnerable. For instance, attacks on any of a large number of buses and

This WORKING PAPER is part of the 2006-CTR-PACER project on the *Five Dimensions of Homeland Security*.

DO NOT CITE WITHOUT EXPRESS AUTHORIZATION FROM THE CENTER FOR TRANSATLANTIC RELATIONS AND THE AUTHOR(S). Contact: transatlantic@jhu.edu

trains are useful to an attacker that seeks to convey that everyone, anywhere, at any time, is susceptible to attack B that people risk their lives doing the ordinary. Even isolated attacks on anonymous individuals can have enormous terror-producing effects, as the 2002 sniper attacks in Washington, DC show convincingly. As always, the problem for the defender is that it can try to protect what it values most but this is wasted effort if the attacker=s interests center on another target, that the defender also values.

Second, terrorists can choose to attack less protected targets when defensive commitments create offensive opportunities. By defending certain targets at the expense of others, the defender redirects the terror threat toward “softer” targets. This target shift is evidenced in Iraq when insurgents moved from attacking less vulnerable US targets (e.g., bases, convoys, and targets in Baghdad=s walled green zone) to Iraqi civilians, recruiting centers, police stations, diplomats, government officials, and Shiite mosques.

When evaluating its capabilities and setting its priorities, then, the defender encounters the long-recognized international dilemma for states seeking to deter attacks on their interests. By designating areas of the world that are in the national interest to defend, a state implicitly excludes other portions of the world from protection and invites attacks on those lesser interests.

Conversely, by claiming lesser interests as “vital,” a state risks depreciating the credibility of its promises to defend any and all of these vital interests if attacked. The credibility of the defender=s claims are at issue in part because of what can be described as a “commitment” problem. The defender can “signal” its terrorist adversaries that it will remain vigilant against any and all terror attacks, as the US did by establishing the Department of Homeland Security and adopting various security reforms. But ambitious commitments invite challenges. The more the defender commits to defend, the greater the challenger=s willingness to test the defender=s resolve and/or capabilities.

Even if terrorists believe that the defender has the *intention* to defend its interests B most certainly true of the defense of targets on national soil B the defender=s credibility is in question when the attacker doubts the defender=s *capability* to respond successfully to an attack. Because the defending government cannot do everything and be everywhere at once, the government cannot devote resources to the protection of targets in proportion to their value. The sheer number of places where large numbers of people congregate B among them, the most vulnerable and sympathetic portions of the population (e.g., school children) B make a universal defense strategy impossible B and dangerous. By attempting to defend more than it can, the defender risks undermining its ability to deter attacks.

Yet the options for the attacker are constrained, as well, given its desire to strike targets of value to a government or society. This limits the range of available choices to targets that governments have a strong interest in defending. Symmetries in value between the attacker and

This WORKING PAPER is part of the 2006-CTR-PACER project on the *Five Dimensions of Homeland Security*.

DO NOT CITE WITHOUT EXPRESS AUTHORIZATION FROM THE CENTER FOR TRANSATLANTIC RELATIONS AND THE AUTHOR(S). Contact: transatlantic@jhu.edu

defender are arguably more the rule than the exception when terrorists desire to hit societies “where they hurt” and to magnify the political, social, and/or economic effects of an attack. Indeed, the evidence is that the impact of so-called spectaculars reverberates beyond the limited threat those attacks present B that people tend to exaggerate the chances that they, too, will be victimized. Because of these very consequences, governments can focus their defenses on what terrorists want to attack. For example, these symmetries arguably abet the US strategy of protecting nuclear power plants more than oil refineries, airline transportation more than bus stations, and the US capital more than other US cities. It also played to the US strategy, immediately after September 11, of concentrating protective resources upon the disarming of airline passengers B preventing them from boarding planes with potential weapons B over screening stowed aircraft luggage for explosives. Assuming that terrorists had less interest in killing hundreds of people when, by hijacking an aircraft and using it as a weapon, they can kill hundreds (perhaps, thousands) of people, destroy a physical structure, and receive credit for pulling off *another* September-11 style attack, the US could focus upon what it regarded as a costly attack scenario.

Although the defender might still be unable to offer a robust defense of the numerous targets that terrorists want to strike, the defender can benefit, as well, from important capability and informational advantages (asymmetries). These limit what the attacker can gain from an attack and/or force the attacker to accept risks and costs in planning and executing an attack. These advantages can boost the credibility of a defender that can capitalize on a variety of (denial-based) strategies.

First, the defender can rely upon a *limited defense*. A limited defense is meant to concede ground B given the prohibitive human and financial costs of a robust defense B and only contain the damage that is suffered in an attack. Viewed from a deterrence standpoint, a limited defense attempts to reduce the value of an attack. The current enforcement of flight restrictions around Washington DC illustrates this. With the high costs of around-the-clock patrols by military aircraft, an identification zone and narrower flight-restricted zone within which aircraft are closely monitored concentrically encircle the US capital. Because it is unlikely, however, that the implementation sequence will unfold within the time period available to shoot down an approaching aircraft or that the order will be given barring extraordinary evidence of hostile intent, the system is best suited to stop a *second attack*, not a first. This limited defense aids deterrence by reducing the value of an attack, that is, by thwarting the catastrophic outcome (i.e., multiple planes crashing into multiple buildings) that motivates the attacker.

Second, the defender can resort to a *partial defense* to boost the costs and risks of an attack. For instance, by reducing key vulnerabilities in high value targets, the defender can deprive the attacker of easy victories and force it to adopt more expensive and dangerous tactics to accomplish its objectives. Simply reinforcing and locking the door to the airplane cockpit, and keeping the door locked under all circumstances, dramatically increases the challenge for an

This WORKING PAPER is part of the 2006-CTR-PACER project on the *Five Dimensions of Homeland Security*.

DO NOT CITE WITHOUT EXPRESS AUTHORIZATION FROM THE CENTER FOR TRANSATLANTIC RELATIONS AND THE AUTHOR(S). Contact: transatlantic@jhu.edu

attacker that seeks to gain control of a passenger aircraft. Indeed, the defender can adopt single measures that reduce the value of an attack *and* increase the costs to an attacker. Protecting critical nodes (e.g., in the electric power grid) or choke points (e.g., railway or highway tunnels) that could produce highly disruptive effects if attacked reduces the payoff from attacking those sites (by offering a limited defense) and forces the attacker to adopt cost-ineffective methods to achieve attack objectives (e.g., attacking electric transmission towers and lines rather than substations).

Third, the defender can utilize a *flexible defense* by allocating resources as needed to blunt an anticipated or actual attack. Consequently, local defenses can be designed only to limit damage from an attack through a “holding action” until reinforcements arrive in the form of light, mobile quick-response military forces, special weapons and tactical (SWAT) teams within police departments, or emergency responders such as hazardous materials teams, medical personnel, fire departments, and help arriving from other municipalities, states, or countries. Flexible defense is also embodied in organizational and/or technological systems that permit a coordinated and informed response to an attack.

Fourth, the defender can resort to a *selective defense* in which resources are allocated to combat more damaging threats rather than less damaging ones. For instance, security is often disproportionately tight at sports events that attract tens of thousands of people. Smaller groupings of people are attractive targets, but the possibility that terrorists could kill and injure a large number of people in a single incident in a celebrated venue makes these events important to defend. Likewise, security can focus on more over less damaging modes of attack. For example, US officials can worry more about a destructive car and truck-bomb threat to homeland civilians and structures than the threat from dismounted suicide bombers.

Fifth, the defender can engage in *defensive screening* efforts in which populations are “filtered,” as they pass through key access points. The intent is to locate those who fit a suspect demographic or behavioral profile and to subject them to additional screening (i.e., searching and/or questioning). Profiling will not work if the size of the suspect population is too large to target for rigorous screening, government agencies focus on physical characteristics at the expense of useful behavioral markers, and members of a “suspect population” retain useful information out of fear that they will inadvertently incriminate themselves, family members, or friends, or damage their community. In principle, though, screening underlies all efforts to monitor the flow of people or goods at some distance from possible targets. For instance, a “profiling” of sorts underlies the US monitoring of container shipments into the US. US customs inspectors focus their scrutiny on “untrusted” shipments from problematic areas of the world and/or that involve importers that have not built a record for clearing customs¹.

¹ Flynn, S. (2004) *America the Vulnerable: How Our Government is Failing to Protect US from Terrorism*, New York: Harper Collins, p. 90

This WORKING PAPER is part of the 2006-CTR-PACER project on the *Five Dimensions of Homeland Security*.

DO NOT CITE WITHOUT EXPRESS AUTHORIZATION FROM THE CENTER FOR TRANSATLANTIC RELATIONS AND THE AUTHOR(S). Contact: transatlantic@jhu.edu

Sixth, the defender can construct a *triggered defense*. The defender need not stay on maximum alert all of the time but can husband resources and go on alert when a possible threat is identified.

Once mobilized, the defender is better able to combat the threat and to appreciate its actual dimensions. Signs of a prison break can trigger a general “lock-down” to counter both the immediate threat (e.g., prisoners who are trying to escape) and unknown other B perhaps, bigger B threats to which the precipitating incident is linked. Similar triggering occurs when a security violation in some US airports leads to an order to “dump the concourse” which requires the re-screening of all airline passengers². Triggering is also involved in decisions to shut-down a subway system when some trains are attacked, to heighten security precautions for all forms of public transportation when one mode is attacked, and to heighten security in US public transportation when the subway system in another country (e.g., Britain) is hit.

Seventh, the defender can engage in a *random defense*. Just as bargaining theories of deterrence relied upon a “threat that left something to chance,” the defender can choose to protect some targets or take some actions periodically and/or unpredictably to increase the risk to the attacker.

The logic of risk manipulation supported the random screening of US airline passengers in the aftermath of September 11. Random screening B let alone the screening of but 1-in-10 passengers B appears to make little sense from a defensive perspective given the severity of the threat should terrorists take control of an airliner. It does make sense from a deterrence perspective (especially if it is assumed that the 10 percent chance of being screened combines with other uncertainties with which the attacker must contend). The 10 percent detection probability is that much more effective as a deterrent if attackers in a group (the 19 hijackers) each have a 1-in-10 chance of being screened and the detecting and detaining of any one attacker will impair or compromise a terror operation. Then, random screening serves a selective defense that focuses on combating a (September-11 style) multiple-attack scenario.

Eighth, the defender can employ the *spatial defenses* that were used in the Cold War-era to strengthen nuclear deterrence. One aspect of these defenses is *mobility*. Just as the nuclear powers relied upon mobile submarines and land-based missiles to keep nuclear forces secure from attack, governments can harness mobility to protect government leaders from assassination. The schedule and movements of the US president are often kept secret and, in times of emergency (e.g., September 11), the president can remain mobile (e.g., Air Force One) or be

² *Ibid*, p. 77.

This WORKING PAPER is part of the 2006-CTR-PACER project on the *Five Dimensions of Homeland Security*.

DO NOT CITE WITHOUT EXPRESS AUTHORIZATION FROM THE CENTER FOR TRANSATLANTIC RELATIONS AND THE AUTHOR(S). Contact: transatlantic@jhu.edu

taken to an undisclosed, fortified location for protection. Another aspect of these defenses is *dispersion* to reduce the value of a *target* (in contrast, a limited defense reduces the value of an *attack*). Just as the nuclear powers chose not to co-locate all of their nuclear resources by creating an inviting target for attack by the US President and Vice President currently avoid attending the same public events. The logic of dispersal underlies recommendations that dangerous chemical facilities be distanced from population centers and that trains carrying dangerous cargos be routed away from urban areas.

Finally, the defender can rely upon *defensive uncertainty*. Despite al-Qaeda's legendary ability to obtain information on targets (through open sources and active surveillance), not all of the strengths and vulnerabilities of a target will be known to an attacker. Available floor plans and maps might be incorrect, dated, or lacking fine details (e.g., the location and capabilities of an alarm system). Or else, uncertainty could arise from unresolved engineering or practical issues that are implicit in an attack scenario. Illustrating this is the considerable controversy about whether the reactor core of a nuclear power plant could survive a direct hit from an aircraft.

Uncertainty could also result from a deliberate policy of defensive concealment. For example, security units seek to multiply their effectiveness by reducing the predictability of their patrol schedules and staffing and by withholding information about their counter-terror tactics and procedures. Inevitably, all partial and flexible defenses have some amount of useful uncertainty built into their performance, unintentionally or by design. A visible airport security presence by though for passenger screening by offers some protection against any and all attacks on airline transportation because the defender *could* stumble onto an attack.

Thus, deterrence can be strengthened when the defender creates favorable capability and informational asymmetries using a number of defensive approaches, alone or in combination. Indeed, deterrence effects could multiply enormously through a packaging of approaches by as illustrated by security at a hypothetical gathering attended by a government leader. The leader can be protected through a selective defense in the form of bodyguards, a full screening of people in close contact with the leader, a partial defense (against certain kinds of attacks) through screening with metal detectors or explosive-sniffing dogs, random screening of all people in attendance, and uncertainty about where the leader will be sitting and how and when the leader will be entering and departing the venue. In combination, these imperfect approaches offer the deterrent advantages of a *layered defense*. The variety of possible combinations of defensive approaches is too large to discuss in full. Suffice it to say that which combinations are usefully employed depends on available defensive resources, the nature and intensity of the threat, and the defender's tolerance for error. Random screening makes little sense if an assassin is known to be in a crowd just as random screening or selective defense of urban targets make little sense if terrorists are known to possess a nuclear weapon that can devastate an entire city.

It is easy, then, to understate the range of options available to the defender and to overstate the

This WORKING PAPER is part of the 2006-CTR-PACER project on the *Five Dimensions of Homeland Security*.

DO NOT CITE WITHOUT EXPRESS AUTHORIZATION FROM THE CENTER FOR TRANSATLANTIC RELATIONS AND THE AUTHOR(S). Contact: transatlantic@jhu.edu

options available to terrorists. Certainly, deterrence is likely compromised should terrorists acquire weapons of mass destruction. The ability of a single atomic bomb to produce widespread destruction at a national point of entry allows an attacker to overcome challenges (e.g., moving the bomb to a distant city) that could undermine operational success. Likewise, a terrorist possessing the anthrax or smallpox virus is arguably positioned to realize a worst nightmare in Western societies and to attack with ease because a biological strain can be introduced surreptitiously into a population. But terrorist groups have not taken full advantage of opportunities to exercise “high-end” options (i.e., spectacularly destructive attacks) or even “low-end” ones that are well within these group=s capability and promise a considerable return. If terrorists have rejected either set of options based on their cost or value, the capabilities of the attacker are inadequate given its objectives, and deterrence is in effect, at some level. Policymakers can magnify these effects with appropriate defensive strategies.

Policy Implications

The principles underlying a denial-based, deterrence strategy are straightforward: “instead of trying to protect every conceivable target against every imaginable form of attack”³, the defender seeks to cause the attacker to accept greater costs and risks and/or a reduced prospect of gain in planning and executing an attack. When governments accept these principles, a number of useful policy guidelines emerge.

First, governments must safeguard their priorities by protecting against *possible* worst-case attacks on national citizens B their lives, livelihood, and property B and *probable* attacks that reflect the goals of the attacker (e.g., the World Bank buildings or Wall Street). In selecting their protective priorities, governments must distinguish the practical value of a target from its patriotic or sentimental value, likely effects from less-likely ones, and short-term consequences of an attack from long-term effects. Thus, a viable strategy could center on protecting transportation links B and airlines in particular given their unique vulnerability B and places in which large numbers of people congregate.

Second, governments can protect targets by conceding their vulnerability. Governments must draw a distinction between tolerable and intolerable levels of destruction. In all likelihood, people will die and/or property damage will occur in a terrorist attack regardless of what

³ Jenkins, B.M. (2002) *Countering al Qaeda: An Appreciation of the Situation and Suggestions for Strategy*, Santa Monica, CA: RAND Corporation, p. 29.

This WORKING PAPER is part of the 2006-CTR-PACER project on the *Five Dimensions of Homeland Security*.

DO NOT CITE WITHOUT EXPRESS AUTHORIZATION FROM THE CENTER FOR TRANSATLANTIC RELATIONS AND THE AUTHOR(S). Contact: transatlantic@jhu.edu

governments and private interests do to prevent it. The operative question must be how best to expend resources to contain and otherwise limit the consequences of an attack.

Third, governments can protect targets by not increasing their vulnerability. Through regulatory efforts aimed at hardening, zoning, transporting, or policing, governments must defend facilities and vehicles that can have devastating collateral effects when struck. Chemical plants and trucks and trains carrying hazardous materials are inviting targets when proximate to urban areas, and these potential “weapons” must be “distanced” from lucrative value targets.

Fourth, governments can protect targets even when doing so incompletely. Defensive measures succeed, controlling for cost, if reducing casualties and damage below levels that would otherwise have occurred.

Fifth, governments must respond, but not over-respond, to threats. Flexible defenses rely upon scarce and depletable resources, and the danger should flexible defenses become static or overused (e.g., through frequent “alerts”) is that they will be unavailable for other contingencies.

Sixth, governments must control national gateways and key corridors of attack. By screening traffic through immigration offices and airports, governments can increase the overall risk to a terror operation that involves large numbers of personnel. Governments must also act to impose risks late in the attack plan. It is one thing to deny entry into a country of an operative whose papers are not in order; it is quite another to nab an attacker at the preparation stage (when guns or explosives are being purchased or specialized training is being sought) or (at a checkpoint) during the execution of an attack. Attackers should not be permitted to assume all risks up front when the security of a terror operation is least likely to be compromised and the penalties for participants are relatively mild (e.g., deportation rather than death in a failed attack).

Seventh, government must adopt covert measures signaled overtly. Covert surveillance can trap a suspect, but a security presence can deter an attack only when advertised. Visible defenses need not be *transparent* defenses: signaling the full capabilities of a defense is advisable only when defenses are impenetrable. Visible devices and procedures that allude, somehow, to the existence of hidden ones are perhaps the best deterrent, for example, in the form of an occasionally strong, albeit somewhat unpredictable, security presence.

Eighth, governments must anticipate new threats but can focus on established ones. Imagining what terrorists *could do* is a useful exercise; but terrorists might have neither the desire nor capability to do what we fear most. This means that governments can capitalize on the learning curve, as terrorist behavior becomes more predictable with time.

Admittedly, a deterrence strategy might not stop all attacks; in fact, it might not stop attacks in

This WORKING PAPER is part of the 2006-CTR-PACER project on the *Five Dimensions of Homeland Security*.

DO NOT CITE WITHOUT EXPRESS AUTHORIZATION FROM THE CENTER FOR TRANSATLANTIC RELATIONS AND THE AUTHOR(S). Contact: transatlantic@jhu.edu

which relatively simple devices are used to kill many people. Unfortunately, deterrence could also cause the attacker to change targets and/or methods resulting in a more damaging attack than the one that had been deterred. But the success of a defense-based deterrence strategy is not assessed by summing the costs; instead, it is assessed by whether, over the long term, the defender is better off with the strategy than without it.

This WORKING PAPER is part of the 2006-CTR-PACER project on the *Five Dimensions of Homeland Security*.

DO NOT CITE WITHOUT EXPRESS AUTHORIZATION FROM THE CENTER FOR TRANSATLANTIC RELATIONS AND THE AUTHOR(S). Contact: transatlantic@jhu.edu